Input Output Research

Cardano Vision & Work Program 2025 Proposal

Version 1.0

Executive Summary

Overview

This document provides an outline of Input Output Research's (IOR) proposal to the Cardano community, via Intersect MBO (Intersect), for Cardano Vision and Work Program 2025. A 2030 vision for Cardano is outlined guided by a research agenda and 5-year program of work. For 2025, IOR is submitting a one year proposal with a $13.42M budget which would deliver a program of work that establishes an annual funnel of 20 fundamental research and 6 technology validation opportunities, deepens our foundational role within the Cardano community, and delivers early research results within a longer term outlook.

Input Output

Founded in 2015 by Charles Hoskinson and Jeremy Wood, Input Output is a pre-eminent blockchain infrastructure research and engineering company. As a fully decentralized, remote organization, we uphold the highest standards of academic rigor and evidence-based engineering. We are proud to support the development of Cardano, driven by our commitment to improving global systems for everyone. Through this work, we've built one of the most passionate and engaged blockchain communities, consisting of developers, stake pool operators, creators, enthusiasts, and lifelong learners.

Cardano & Intersect

Cardano is a proof-of-stake blockchain platform: the first to be founded on peer-reviewed research and developed through evidence-based methods. It combines pioneering technologies to provide unparalleled security and sustainability to decentralized applications, systems, and societies. Intersect is a member-based organization within the Cardano ecosystem, tasked with ensuring its continuity and future development. Bringing members together behind a shared vision, Intersect enables a more resilient, secure, transparent, and innovative Cardano ecosystem that puts members in the driving seat of Cardano's future.

2030 Outlook

To continue to lead in blockchain over the next five years and beyond, Cardano requires a robust research and innovation agenda focusing on scalability, interoperability, security, and sustainability. This includes advances in consensus algorithms, such as Ouroboros Omega, zero-knowledge proofs, quantum-resistant cryptography, and enhanced smart contract functionality. The goal is to address global and societal challenges to create impact, while driving innovation and maintaining high standards of security and efficiency.

Cardano's five-year outlook is outlined through a Strategic Research Agenda which is structured into two 2.5-year Vision phases with a mid-term review, and organized into consecutive annual and biannual Work Programs as outlined in Figure 1 below. Each Work Program includes specific workstreams with tasks, milestones, and deliverables, all aimed at delivering excellence, quality and implementation. This agenda

builds on Cardano's track record of 100% uptime, ensuring continuous improvement and maintaining its position at the forefront of blockchain technology.

Figure 1. 2030 Outlook for Cardano 2.0

Strategic Research Agenda

The blockchain industry, including Cardano, stands at a pivotal moment requiring extensive research and development (R&D) to fulfill its transformative potential. IOR proposes a Strategic Research Agenda (SRA 25/29) for the period 2025–2029, anchored in an Evidence-Based Methodology that ensures transparency, security, and rigorous validation through formal methods and peer-reviewed scientific processes.

Since Cardano's inception, Input Output has pioneered foundational and applied research, resulting in a robust intellectual repository comprising over 200 peer-reviewed publications cited more than 10,000 times. Approximately 50 of these publications directly underpin Cardano's developmental milestones, enabling substantial technological advancements and industry leadership.

IOR's mission addresses three core challenges faced by the blockchain ecosystem:

- **Sustainability**: Enhancing and maintaining energy-efficient, socially responsible practices, continually aligning blockchain technology with positive environmental and societal impacts.
- **Scalability**: Advancing the ability of the blockchain to efficiently handle increased global transaction volumes and decentralized application demands without sacrificing performance.
- **Interoperability**: Developing robust standards and protocols that facilitate seamless cross-chain communication and collaboration, vital for building an interconnected blockchain ecosystem.

IOR has supported Cardano to outline a set of fundamental blockchain tenets, akin to a bill of rights, that a robust blockchain infrastructure must fulfill to achieve the goals envisioned by the industry since its

inception 15 years ago. Every blockchain system, or any proposed enhancement to it, is evaluated against these tenets to determine how well it supports or aligns to them.

IOR operates under the scientific leadership of Chief Scientist Aggelos Kiayias FRSE, coordinating over 30 globally distributed research fellows and a dedicated Technology team of more than 35 engineers, tasked with swiftly validating and prototyping advanced research concepts. Central to IOR's strategy is its **Evidence-Based Methodology**, ensuring systems are underpinned by rigorous formal proofs, thorough validation, and precise specifications. This meticulous approach allows high-quality, high-assurance innovations, with clear transition paths from research to deployment, to support long-term development and growth.

Implementation and monitoring of the SRA 25/29 will follow structured Work Programs with clearly defined KPIs, regular stakeholder engagement, and adaptive feedback mechanisms. This structured approach facilitates strategic alignment, operational resilience, educational initiatives, and broad ecosystem adoption. Ethical conduct and research integrity form foundational pillars of IOR's approach, ensuring trust, transparency, and societal benefit, reinforcing Cardano's global leadership and its capacity to consistently deliver fundamental, lasting value.

Cardano Vision

IOR's five-year vision for Cardano is structured in two 2.5-year phases (P1 and P2) with a mid-term review. This vision for Cardano, which outlines priorities, objectives and proposed application areas, is informed by Cardano's tenets, analysis of the research landscape and stakeholder consultations, reflecting on lessons learned over the past five years to ensure Cardano remains competitive and widely adopted.

Cardano Vision aims to enhance Cardano's capability through 9 thematic focus areas outlined below. By focusing on these targeted areas, Cardano aims to further its market-leading research portfolio, reinforce its status as the foremost blockchain within the research community, and provide product and engineering teams from the community with a continuous funnel of commercialization opportunities in the most relevant and innovative focus areas.

(i) The World's Operating System

To support decentralized applications and digital assets at scale, Cardano must offer powerful, secure, and feature-rich smart contract capabilities. This enables value transfer and more complex interactions, such as DeFi, while maintaining performance and security.

(ii) Ouroboros Omega

As Cardano's proof-of-stake consensus protocol, Ouroboros provides energy efficiency and resilience. However, continued research is needed to meet rising demands for throughput and performance as the network scales.

(iii) Tokenomicon

Tokenization powers value representation on blockchain. Cardano leads with features like native assets and Babel fees, but the economic models that underpin token ecosystems remain underexplored. This stream focuses on rigorous tokenomics research and design.

(iv) Global Identity

Decentralized identity empowers users with privacy-preserving, user-centric, and interoperable digital credentials. Research here aims to define the foundations of a global identity system and integrate it within the Cardano ecosystem.

(v) Democracy 4.0

Building on historical evolutions of democracy, this stream explores how blockchain can support scalable, inclusive, and secure governance mechanisms, adapting democratic processes to meet 21st-century challenges.

(vi) The Internet Hydra-ted

Hydra is Cardano's state-channel suite for layer 2 scalability. While the Hydra Head is deployed, full functionality requires continued R&D to enable high-performance, low-latency applications comparable to Web2 platforms.

(vii) Interchains

Interoperability across blockchains and external systems is critical but comes with major security challenges. This stream develops evidence-based, minimal-trust mechanisms to securely connect Cardano to other ecosystems.

(viii) Core Zero-Knowledge Capabilities

Zero-knowledge proofs (ZKPs) are key to privacy and efficiency. Cardano needs modular, updatable ZK tooling that supports applications like light clients, state proofs, and bridges—keeping pace with rapid advances in ZK research.

(ix) The Post-Quantum Landscape

Quantum computing threatens today's cryptographic foundations. This stream focuses on replacing vulnerable primitives and designing quantum-secure consensus and key management systems—while also exploring quantum-enhanced blockchain capabilities.

Work Programs

The Strategic Research Agenda is organized into three to five consecutive Work Programs, each detailing workstreams within the nine thematic focus areas. These include objectives, tasks, deliverables, and resource allocation for specific research and technology validation streams. The programs aim for technical and scientific excellence, focusing on prototype validation in both simulation and test

environments. The goal is to advance research, develop scientific foundations for breakthrough technologies, and validate applications for market readiness, supporting business model innovation and scaling.

This rigorous system-building approach is driven by the tenets outlined in the Smart Research Agenda and thematic focus areas defined in the Cardano Vision. IOR works closely with the Intersect Product Committee and other Cardano community stakeholders to invite feedback and discussion. This ensures development is relevant, iterative, and adaptive, allowing artefacts and software to evolve over time, whilst ensuring each work programme is thoroughly evaluated for quality and impact.

Work Program 2025

The $13.42M total budget for WP25, allocates $5.895M for Fundamental Research and $7.525M for Technology Validation, is for a total of 56.1 FTEs. This includes 20 fundamental research and 6 technology validation streams, all aligned with Cardano Vision. Each stream is evaluated at launch and throughout its development, with a focus on tangible outputs such as peer-reviewed publications, technical reports, prototypes, and specifications. As deliverables emerge, priorities are adjusted to align with Cardano's strategic goals and evolving opportunities.

Prioritization balances market relevance, methodological rigor, and available resources. While foundational research may not track rapid market trends, the focus is on first-principles inquiry—deep, long-term exploration that delivers lasting impact. From over 20 annual research opportunities, 6 high-impact innovations are selected for technology validation and implementation, through a rigorous, multidisciplinary process involving community, customer, and R&D input.

Fundamental Research

World's Operating System

- **State-Machine Contract Environment (WOS-2):** This stream simplifies the formal description of smart contracts for Cardano through a formal state-machine framework (EasySM) that abstracts the complexities of the EUTxO model and facilitates verification.

- **Location-Based Services and Smart Contracts (WOS-6):** This stream explores how geolocation can enhance smart contracts and node infrastructure, focusing on geographic diversity metrics and incentives for global decentralization.

Ouroboros Omega

- **Ouroboros Peras – Vision (OO-1V):** A first version of Peras has been delivered, showing promising improvements in settlement times, with ongoing research focused on enhancing robustness and avoiding cooldown phases for greater efficiency.

- **Ouroboros Leios (OO-2):** Leios introduces vertical scalability to Cardano's consensus by aligning throughput with node resources, overcoming current limitations in block size and timing.

- **Fair Transaction Processing (OO-3):** This stream develops protocol-level solutions to reduce

front-running issues and ensure fair transaction ordering, reducing MEV without compromising decentralization or performance.

- **Multi-Resource Consensus – Minotaur (OO-5):** Minotaur explores hybrid consensus mechanisms that combine PoW and PoS (including restake from different PoS networks) to improve security, resilience, and inclusivity—features that further help bootstrapping low-liquidity or early-stage blockchains that rely on Cardano for security.

- **Proofs of Useful Work (OO-6):** This stream advances consensus models that replace wasteful PoW with verifiable, valuable computation ((including SAT solving, zk-SNARK generation, ML computation, etc.), building on Ofelimos to enhance sustainability and network utility.

- **Congestion Control (OO-7):** This research reimagines blockchain fee models by introducing resource- and urgency-based pricing to ensure fair, predictable, and efficient transaction processing under network load.

Tokenomicon

- **Tokenomics Design (TO-1):** This stream develops mathematical models to guide Cardano's long-term macroeconomic policies, optimizing token circulation and ensuring system stability through evidence-based parameter choices.

- **Rewards Sharing and Transaction Fees (TO-2):** Focused on fair and effective incentive design, this stream seeks to improve reward distribution and fee mechanisms to support decentralization, user fairness, and platform competitiveness.

Global Identity

- **Decentralized Identity and Reputation (GI-1):** This stream designs a formal, flexible identity framework enabling users to control and share digital credentials securely across platforms, supporting cross-application interoperability and the effective use of identities in protocols.

Democracy 4.0

- **Next-Level Governance Protocols (D4-1):** This workstream develops scalable, decentralized governance systems with secure, low-footprint voting mechanisms suited for future growth and aligned with Cardano's constitutional principles.

- **Governance Incentives (D4-2):** Focused on DReps and beyond, this stream designs incentive schemes that balance effective decision-making with decentralization, transparency, and fairness in Cardano's evolving governance landscape.

Internet Hydra-ted

- **Hydra Tail (IHT-1):** Hydra Tail enhances Cardano's layer 2 scaling with zk-rollups, enabling off-chain transaction batching and secure on-chain settlement through succinct zero-knowledge proofs.

- **Inter-Head (IHT-2):** This stream extends Hydra to support scalable, multi-party state channels that enable fast, composable layer 2 interactions with minimal on-chain footprint.

- **Optimization Tools (IHT-3):** Focused on Hydra network efficiency, this stream develops tools for fund rebalancing, message routing, and synchronization to maximize throughput and resource use.

- **Auditing Tools (IHT-4):** This stream introduces optional auditing features for Hydra to balance privacy with accountability, enabling limited, compliant access to off-chain transaction history for institutional clients.

Interchains

- **Light Client Infrastructure (IC-3):** Develops secure, efficient, and incentivized light clients to support scalable applications like zk-bridges, addressing device limitations and data asymmetry.

- **DApps Tokenomics (IC-4.1):** This research explores tokenomics principles for launching new dApps or partnerchains, focusing on early-stage design for economic stability and adoption.

- **Consensus Innovation (IC-4.2):** This stream investigates next-generation consensus protocols—blending Nakamoto and BFT models—to enhance Cardano's scalability, decentralization, and fault tolerance under dynamic network conditions.

Technology Validation

- **TV-1. Leios:** This stream advances Ouroboros Leios toward implementation by formalizing specifications, modeling performance, analyzing security, and preparing a CIP for high-throughput, real-world deployment on Cardano.

- **TV-2. Anti-Grinding:** Focused on reducing settlement times, this stream strengthens anti-grinding protections in Praos and related protocols to increase adversarial costs and improve security.

- **TV-3. Jolteon Liveness:** A new high-performance BFT consensus protocol for Partnerchains, delivering formal safety guarantees and competitive finality.

- **TV-4. RSnarks:** Enabling scalable, privacy-preserving zk-bridges via recursive SNARKs by adapting Halo2 proofs for Cardano verification, enhancing interoperability with other blockchains with foreign pairing check and building Plutus-compatible tooling.

- **TV-5. Proof of Restake:** This stream supports secure blockchain launches using hybrid consensus, enabling validators to re-stake from other chains and transition to native stake as adoption grows.

- **TV-6. Light Clients Infrastructure:** Aims to enable efficient, low-resource wallet and smart contract interaction, with ongoing research focused on a novel blind signature-based protocol to support decentralized, DApp-friendly infrastructure.

Summary

Input Output, one of the three pioneering entities behind Cardano, was initially contracted to design, build, and maintain the Cardano platform. This foundational role has positioned IOR at the heart of Cardano's ongoing innovation and evolution, making it a key driver of the platform's future growth and success. Our ambition is to surpass your expectations as a trusted partner, enabling the success of the Cardano community over the next 5-10 years through an unparalleled pursuit of research and technical excellence.

This proposal defines a vision of Cardano over a five year timeline and a supporting budget. Central to this vision is a focus on fundamental research, a core strength of Cardano and key differentiator when compared to other blockchains. With over 200 research papers already contributing to this foundation, the proposal outlined ensures a continuous stream of commercialization opportunities that place Cardano at the forefront of blockchain innovation.

Contents

Who Should Read This Document

This document is a valuable resource for DReps, the Constitutional Committee, SPOs, and all other community stakeholders interested in Cardano.

This Strategic Research Agenda defines a vision for Cardano over a 5 year timeline, and supporting budget, to establish a world leading blockchain and ecosystem across 3 layers. The document offers a comprehensive overview of the strategic initiatives that will shape Cardano's market positioning and community engagement efforts. The IOR proposal outlines the strategic allocation of resources by IOR to drive research and innovation across nine thematic focus areas.

Cardano Vision plan serves as an interface between the overarching Strategic Research Agenda and specific workstream activities set out in each of the consecutive work programs. It provides planning stability beyond the customary 1-2 year period of work programmes, and builds in flexibility to respond to unforeseen challenges and new opportunities as the broader blockchain landscape evolves.

Each Work Programme defines the individual research and innovation workstreams within nine thematic focus areas. DReps and the Constitutional Committee will find this document provides details of Cardano's research and innovation activities for the current year. This alignment ensures that all activities are geared towards delivering high-impact technologies that have the potential to scale and support Cardano’s growth and leadership.

1. Strategic Research Agenda 25/29

1.1 Introduction

Cardano is a proof-of-stake blockchain platform: the first to be founded on peer-reviewed research and developed through evidence-based methods. It combines pioneering technologies to provide unparalleled security and sustainability to decentralized applications, systems, and societies. Built by a leading team of engineers, Cardano exists to redistribute power from unaccountable structures to the margins – to individuals – and be an enabling force for positive change and progress.

Each developmental era, backed by academic research, has been marked by a commitment to advance blockchain capabilities in the following areas:

1. Byron - Establishing a robust foundation for the network
2. Shelley- Decentralizing the ecosystem to empower users
3. Goguen - Embedding smart contract functionalities to expand its applications
4. Basho - Enhancing scalability to accommodate increasing demands
5. Voltaire - Incorporating decentralized governance mechanisms

This visionary mission to evolve Cardano into a fully self-sustaining and adaptable blockchain ecosystem is designed to service its global user base's diverse and changing needs.

1.2 Background

As Cardano enters the Voltaire era of its roadmap, research continues to play a central role—as it has throughout each phase of Cardano's development. Since Cardano's inception, IOR has performed fundamental and applied research across a wide array of open questions in blockchain systems. This has enabled timely access and subsequent development within the Cardano community by disseminating research outputs freely. Whilst contributions to peer review, conference sponsorship and organization has supported broader research efforts beyond the publication of papers.

IOR is structured around some key themes and it is important to understand how these have shaped the Cardano eras:

- Consensus (Ouroboros, Bryon & Shelley)
- Game Theory & Economics (Ouroboros)
- Sustainability & Governance (Voltaire)
- Expressibility & Programmability (Plutus & Marlow, Gougen)
- Performance & Scalability (Basho)
- Networking (communication across the systems) (Basho)
- Privacy and Identity (Voltaire)
- Interoperability (Basho)
- Regulatory Tech (Voltaire)

Currently IOR's library contains over 200 peer reviewed and published papers, involving over 150 academics, and which collectively have been cited over 10,000 times. Of these, around 50 papers are core to the five development phases of Cardano, providing the foundational research that has enabled Cardano to exist in the form it does today.

1.3 Mission

Like other Blockchains, Cardano faces several key challenges as it strives to achieve widespread adoption and technological maturity.

- **Sustainability:** While Cardano's proof-of-stake model is more energy-efficient than traditional proof-of-work systems, the platform must continuously assess and improve its sustainability practices. This involves ensuring that its network infrastructure, development processes, and community initiatives contribute positively to the environment and society, aligning technological progress with broader impact.

- **Scalability:** While Cardano's proof-of-stake consensus mechanism, Ouroboros, is designed to be more scalable than traditional proof-of-work systems, the platform must continue to evolve to handle increasing transaction volumes and decentralized applications (DApps) without compromising speed or efficiency. Ensuring that the network can scale effectively to meet the demands of a global user base is a critical ongoing task.

- **Interoperability:** For Cardano to achieve its vision of a more connected and interoperable blockchain ecosystem, it needs to establish seamless communication and integration with other blockchain platforms. This involves developing robust protocols and standards that facilitate cross-chain transactions and data exchange, which is complex and requires broad industry collaboration.

1.4 Tenets

The blockchain industry, including Cardano, is at a point where advancing research and development in several key areas is essential to deliver the blockchain industry's promise to the world. Input Output has supported Cardano to outline a set of fundamental blockchain tenets that a robust blockchain infrastructure must fulfill to achieve the goals envisioned by the industry since its inception 15 years ago. Every blockchain system, or any proposed enhancement to it, is evaluated against these tenets to determine how well it supports or aligns with them.

- **T1** *your transaction cannot be slowed down or censored and will be expediently served for its purpose* (system must scale - throughput, sharding, settlement and dynamically price, layer 2)

- **T2** The cost of a transaction should be predictable and cannot be unreasonable *(system should facilitate an accessible predictable pricing)*

- **T3** You will not be prevented from developing and deploying your application as you intended it *(system should offer DSLs and formal verification support, pub/sub location services, oracles, partnerchains)*

- **T4** Your contributions to the system will be recognized, recorded and assessed fairly *(rewards sharing for SPOs, tokenomics, multi-resource consensus)*

- **T5** The system will not lock the value that you store in it without your consent_ *(interoperability, partnerchains)*

- **T6** The system will safely preserve the value and information that you decide to store in it *(integrity, post-quantum security, decentralization, decentralized storage, stablecoins, key management, ownership)*

- **T7** The system will not unnecessarily spend resources *(proofs of useful work, efficient design, memory, storage)*

- **T8** The system will treat users equally and will evolve according to their collective will aiming at its long term sustainability and viability *(fairness, neutrality, sustainability, governance, decentralized identity, multi-resource consensus, democracy 4.0)*

- **T9** The system will preserve the privacy of the users' actions to the degree that is possible while facilitating the other tenets *(privacy preserving techniques for identity, secure MPC)*

- **T10** The system will offer users ways to engage that do not require them to break local laws and regulations to the degree that is possible while facilitating the other tenets *(regulatory compliance, RVTP)*

- **T11** The dynamics of the system shall be transparent, open, verifiable and interpretable to the degree that is possible while facilitating the other tenets *(transparency, democracy 4.0)*

1.5 Scientific Leadership

IOR is led by Chief Scientist Aggelos Kiayias FRSE and encompasses two departments within Input Output; a Research network of over 30 distributed research fellows and operational staff who strive for the highest standards in academic excellence and applied research, and an Innovation team of more than 35 engineers split into six smaller teams that focus on rapid prototyping and validation.

The research department includes an office of three staff, who support Aggelos operate an in-house team that includes 10-15 research fellows specializing in areas such as cryptography, distributed ledgers, algorithms, cybersecurity, formal methods, economics, and game theory. In addition, the research department works closely with more than 20 external researchers embedded across a network of academic partnerships with prestigious universities worldwide.

Within the innovation department, each sub team consists of 6 or more and can include a product manager, technical architect, prototyping (software) engineer, applied cryptographer, research liaison and formal methods engineer. These resources are allocated to specific innovation work streams depending on the success criteria required to achieve the desired outcome for implementation..

Chief Scientist

Professor Aggelos Kiayias FRSE is the Chief Scientist at Input Output and directs the organization's pioneering research in blockchain and cryptography. He holds the Chair in Cyber Security and Privacy and serves as the Director of the Blockchain Technology Laboratory at the University of Edinburgh. His research interests encompass computer security, applied cryptography, and distributed systems, with a particular focus on blockchain technologies, e-voting, secure multiparty protocols, privacy, and identity management.

Professor Kiayias has been instrumental in the development of Cardano's Ouroboros protocol, a cutting-edge proof-of-stake consensus algorithm, and is widely recognized for his contributions to the advancement of secure and scalable blockchain protocols. In 2021, Kiayias was elected a Fellow of the Royal Society of Edinburgh, and in 2024 he was awarded the BCS Lovelace Medal recognizing his transformative contributions to the theory and practice of cybersecurity and cryptography.

Blockchain Technology Laboratory

The Blockchain Technology Laboratory network consists of three academic partners and was created in 2016 through the initiative of Input Output to carry out industry-inspired open access research in blockchain technologies and decentralized systems in collaboration with industry and government partners.

The University of Edinburgh, UK serves as a leading research center focused on advancing blockchain technology. With a strong emphasis on cryptography and distributed systems, the lab is at the forefront of developing secure and scalable blockchain protocols, contributing significantly to the Cardano ecosystem. The team comprising professors, lecturers, postdocs and PhD students who are involved in several projects including:

- The Edinburgh Decentralisation Index (EDI) studies blockchain decentralization from first principles, archives relevant datasets, develops metrics, and offers a dashboard to track decentralization trends over time and across systems.

- ZK Lab: advancing the frontiers of zero-knowledge protocols, ensuring utmost privacy without compromising on security or performance.

Institute of Science Tokyo (formerly Tokyo Tech), Japan is a prestigious institution known for its cutting-edge research in engineering and technology, including blockchain. Its research initiatives in blockchain focus on smart contracts, security, and scalability, fostering innovation in both academic and industry applications.

University of Wyoming, USA is a leader in blockchain education and research, with initiatives like the Blockchain Center of Excellence driving advancements in the field. The university collaborates with

industry and government partners to explore applications in finance, supply chain, and digital identity, positioning Wyoming as a hub for blockchain innovation.

1.6 Evidence-Based Methodology

Achieving correctness, security, and reliability is inherently challenging. It requires examining a system under all possible circumstances, which is an infeasible task given that this cannot be demonstrated experimentally. This is particularly relevant for distributed, decentralized systems which are run by volunteer community members, on a global scale, on public infrastructure.

For precisely this reason, mathematical models, proofs, and formal methods are required to obtain high assurance. To achieve this, IOR's **Evidence Based Methodology** is rooted in peer reviewed science. This ensures a strong connection between design and implementation throughout the research and innovation process, and leads to high quality systems that we can confidently continue to build on and evolve over the longer term.

Agile Approach

High assurance is critical in Web3. Beyond protecting monetary systems, decentralized platforms lack centralized governance, making rapid fixes difficult in the event of failure. To minimize risks, solutions must meet exceptionally high standards—supported by peer-reviewed papers, specifications, and executables that enable expert verification and challenge.

While rigorous, IOR's approach is flexible and iterative, contrasting with rigid, linear models like waterfall. In static processes, bugs or feature requests can undermine the entire chain of evidence. Our adaptive method enables early identification of roadblocks, efficient resource use, and continuous evolution of both artifacts and software—ensuring robust, reliable systems without compromising integrity.

Software Readiness Levels

Software Readiness Levels (SRL), inspired by and historically referred to as Technical Readiness Levels (TRL), were developed to provide a simple, standardized and systematic method for assessing the maturity of systems, whilst understanding the cost, schedule and risk associated with development.

The SRL scale outlined below provides a means of relative comparison to allow for fair and analogous reviews to enable decision making to assess and communicate the maturity level of a technology throughout its research, innovation (or development) and implementation (or deployment) phased progression.

Research to Proof-of Concept - fundamental ideas are explored and basic concepts are demonstrated, though they may not yet be integrated into the subsequent development

- **SRL1** – Basic principles observed and reported:
  The problem statement has been formulated and the potential solution identified.

- **SRL2** – Technology concept or application formulated:
  A technical solution has been formulated, and paper-and-pencil proofs of its properties have been written.

Innovation & Technology Development - progression from basic functionality toward a prototype that can be validated under more realistic conditions.

- **SRL3** – Analytical and/or experimental critical function or characteristic proof-of-concept:
  A simulation of the solution and its environment has been developed, and the key properties are replicable.

- **SRL4** – Component validation in a simulated or controlled environment:
  A working prototype of the proposed solution has been developed, including the detailed logic, and the identified properties still hold.

- **SRL5** – Component validation in a relevant environment:
  The transition from a simulated environment to a test environment has been completed, and the key properties continue to hold.

Technology Implementation & Delivery - deploying the software in an operational environment and validating its performance under real-world conditions.

- **SRL6** – System/subsystem model or prototype demonstration in a relevant environment:
  The solution is integrated into the target system and interacts with it flawlessly in a test environment.

- **SRL7** – System prototype demonstration in the target environment:
  The prototype can be deployed in the target environment, and its behavior can be observed.

- **SRL8** – Actual system completed and qualified through test and demonstration:
  An actual solution is developed and behaves according to the specifications, with the conformance tests defined in the prototype successfully verified.

- **SRL9** – Actual system proven through successful mission operations:
  The final solution is deployed and behaves according to the specification in the production environment.

Within IOR the research and innovation teams work collaboratively through the Proof of Concept and Development phases to mature the technology or software readiness level of a solution from a basic idea (SRL0) to component validation or prototype validation (SRL4-5) depending on the implementation requirement for the software to be delivered by product teams within the Cardano ecosystem and the customers they are piloting with.

Formal Methods

A rigorous research and development process begins with a well-defined formal model, serving as the definitive reference for researchers, architects, and engineers. This model ensures a unified understanding of design and, as the project evolves, expands into a complete specification that details design elements and identifies key implementation attributes.

The model should be established early in the process and kept lightweight during periods of design flux. Later, it facilitates confident modifications by clearly revealing dependencies and trade-offs. Early performance modeling confirms design feasibility and uncovers potential issues, saving development effort down the line.

A high-quality formal model balances abstraction with precision, focusing on essential design aspects while aligning with ongoing research and prototyping. Ideally, it is executable—serving as both a specification and a reference implementation for prototype testing. Our approach to modeling is tailored to each project, prioritizing aspects based on potential impact.

To support formal model development, we leverage and contribute to advanced theorem provers like Agda and Lean, alongside other specialized tools and techniques that accelerate and refine the formalization process.

Innovation Funnel

This Evidence-Based Methodology serves as a structured funnel to guide research from early exploration to market readiness. Each stage of the funnel increases the maturity of a workstream, reducing uncertainty and aligning outputs with real-world use cases, ultimately supporting successful technology adoption.

This methodology is key to driving impact within the Cardano Vision program and is expected to generate over 100 high-quality research outputs. From these, approximately 30 streams will be selected for technology validation, preparing them for implementation on Cardano's Testnet and Mainnet. This funnelled approach ensures that innovation is both scientifically sound and technically feasible, accelerating the delivery of transformative capabilities to the Cardano ecosystem.

1.7 Fundamental Research (up to SRL2)

Researchers at Input Output develop and formalize novel ideas that go beyond the current state of the art. This process defines clear requirements, identifies trade-offs or limitations, develops meaningful mathematical models, sets design goals, and proposes technically sound solutions supported by rigorous security proofs.

Once the core idea and expected benefits are defined, researchers produce pseudocode and a technical report. The goal is to create a scientific artifact—typically a paper for peer review—that demonstrates the solution's mathematical soundness under well-defined assumptions.

The focus is on solving open research problems relevant to Cardano or its ecosystem. Duration varies by topic and complexity. Early stages may involve only researchers or include collaboration with stakeholders and engineers to extract use-case-specific requirements. As the solution matures, formal methods may be applied to verify properties, with support from formal method engineers as needed.

Formalization typically results in a technical report or research paper (draft or final), and potentially a formal specification—key outputs for transitioning into the prototyping phase. To accelerate this, researchers are encouraged to share work early, prioritizing technical reports when appropriate.

- **Problem Statement:** The process begins with clearly defining the problem and identifying both functional and non-functional requirements. This shapes the research direction and ensures clarity on goals and constraints.

- **Abstraction and Formal Modeling:** The problem is abstracted into a formal model, focusing on relevant aspects and documenting assumptions and boundaries. This helps determine feasibility and identify necessary refinements if dead ends arise.

- **Solution Design and Security Proofs:** A solution is designed within the formal model, and security properties are mathematically proven under stated assumptions. This step assesses feasibility and may require adjustments to the model or assumptions.

- **Documentation and Peer Review:** The research is compiled into a structured paper for peer review, ensuring rigor and validity. Peer-reviewed outputs enhance trust in the findings and may be shared through Cardano Improvement Proposals (CIPs) or Intersect working groups.

1.8 Technology Validation (up to SRL5)

This technology validation phase bridges the gap between research and implementation, led by the Innovation team in collaboration with engineering and product. Over 6–12 months, the team validates research assumptions in practical environments and defines the technical specifications needed for deployment. Close collaboration with the research team ensures clarity on the artifact, with feedback loops established to refine the solution if design limitations emerge.

All reference documentation is maintained alongside the prototype in a shared repository. Implementation teams and relevant stakeholders are engaged early to raise integration concerns and estimate effort, supporting a smooth transition into the target environment.

The prototyping phase should yield the following documents:

(i) A formally verified reference implementation
(ii) A functional prototype for test/simulated environments
(iii) Conformance tests and benchmarks (from formal specs or handcrafted)
(iv) A requirements document detailing what and why
(v) A Cardano Improvement Proposal (CIP) outlining the solution and implementation path

Upon reaching the required SRL level, agreed with the implementation team, the solution proceeds through conformance testing and final validation. Once deployed, the artifact's properties are verified in the production environment. If discrepancies arise, research and innovation teams collaborate with stakeholders to assess whether the deviations are acceptable or require adjustments.

- **Formal Verification:** The goal is to produce a precise, executable specification that captures critical properties like correctness, security, and timeliness. For consensus protocols, this includes proving safety, liveness, and correctness through formal methods. Executable specifications support continuous testing and validation throughout development.

- **Prototypes and Simulations:** Prototypes are developed early to explore design trade-offs and uncover practical challenges. These may run in simulated environments and are used to validate feasibility, performance, and implementation risks. Conformance testing, such as property-based testing, links the prototype back to the formal model and validates performance through benchmarks.

- **Specifications and CIPs:** Specifications offer a definitive, technical description of the design, serving as both a communication tool and acceptance criteria for implementation. CIPs provide a community-facing summary that justifies proposed changes, supported by prototypes, specifications, and performance data.

- **Tooling:** Effective tooling is essential for collaboration across disciplines. IOR uses a mix of off-the-shelf tools and in-house developments, often aligned with production tools (e.g., Haskell, Rust, Agda). Tools like Agda, agda2hs, agda2rust, DeltaQ, QuickCheck Dynamic, Lean, and netsim support formalization, testing, and simulation.

1.9 Operations & Reporting

The Cardano Vision five-year research and innovation strategy is outlined in this Strategic Research Agenda, structured around a Cardano Vision plan delivered in two phases, with a mid-term review. It is implemented through consecutive Work Programs with (bi)annual budgets. Each program includes defined workstreams with descriptions, KPIs, tasks, and deliverables focused on operational resilience, education, and adoption.

IOR's approach to evaluation, reporting, and monitoring aligns with the overall strategic direction while allowing flexibility through periodic reviews and stakeholder consultation. It establishes clear feedback loops between Intersect, IOR, and other Cardano stakeholders to ensure consistent, coherent, and efficient responses to outcomes.

Impact measurement will evolve over future programming periods, incorporating lessons learned and experience gained. A reporting and monitoring framework will include KPIs for administrative expenditure, results, and common data models. IOR, Intersect and interested community members will co-design relevant tools and indicators for impact tracking, including interim reviews and final reporting procedures as detailed below:

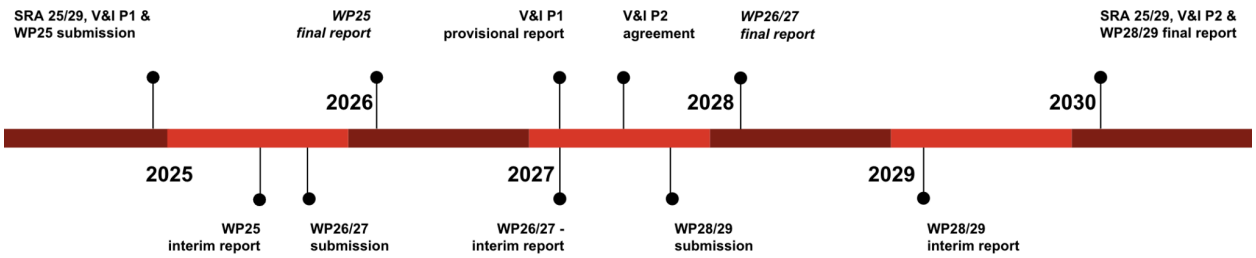

Figure 2. Submission & Reporting Timeline

- **Oct 2024 (Delayed): SRA 25/29, V&I(P1) and WP25 - submission and agreement:** Formal proposal submission for approval, including budgetary requests, following a 3 month consultation with Intersect and Cardano stakeholders

- **July 2025: WP25 - interim report:** A 6 month report outlining early research results and communicating priorities / focus areas ahead of WP26/7 and submission.

- **Oct 2025: WP26/27 - submission:** Formal proposal submission of WP26/7 following consultation with Intersect and Cardano stakeholders.

- **Feb 2026: WP25 - final report:** *Formal report summarizing workstream statuses, progress on tasks / deliverables and budget expenditure to close WP25.*

- **Jan 2027: WP26/27 - interim report, V&I(P1) - provisional report:** A 1 year report outlining research results and workstream statuses for WP26/27 and a V&I(P1) provisional report kicking off a 3 month mid-term review.

- **July 2027: V&I(P2) - agreement:** Formal announcement of the updated V&I(P2) agreement with Intersect and Cardono stakeholders.

- **Oct 2027: WP28/29 - submission:** Formal proposal submission of the WP28/9 following consultation with Intersect and Cardano stakeholders.

- **Feb 2028: WP26/27 - final report:** *Formal report summarizing workstream statuses, progress on tasks / deliverables and budget expenditure to close WP26/27.*

- **Jan 2029: WP28/29 - interim report:** A 1 year report outlining research results, workstream statuses and forecast deliverables for WP28/29 ahead of the SRA end of year closure.

- **Feb 2030: SRA 25/29, V&I(P2), WP28/29 - final reporting:** *Formal program closure.*

1.10 Boosting Cardano

IOR plays a central role in advancing Cardano by supporting core platform development, guiding new ventures, and amplifying the impact of ecosystem projects. From initial concept to deployment, IOR leverages deep expertise to help projects navigate critical stages of growth. This support extends beyond R&D to education, community-building, and fostering a collaborative environment for developers, researchers, and enthusiasts.

Core Contributions

IOR plays a pivotal role in supporting Cardano, ensuring it remains a leading blockchain platform capable of meeting the evolving needs of its global user base.

- **Protocol Innovation:** IOR is behind the design of Cardano's foundational technologies, including the Ouroboros proof-of-stake protocol, which set new standards for security, scalability, and energy efficiency through rigorous academic research and peer review.

- **Scalability & Performance:** Layer 1 enhancements like Leios and layer 2 solutions such as Hydra boost Cardano's throughput, enabling support for high-volume decentralized applications while preserving security.

- **Smart Contracts & Governance:** Through developments like the Chang upgrade and Conway ledger era, IOR has advanced Cardano's smart contract functionality and introduced decentralized governance, empowering ADA holders to shape the platform's future.

- **Security & Formal Methods:** IOR prioritizes high-assurance engineering, using formal verification to mathematically ensure the correctness and safety of protocols, minimizing vulnerabilities and enhancing trust.

- **Interoperability & Standards:** By developing open standards and interfaces, IOR enables Cardano to interact seamlessly with other blockchain networks, expanding use cases and cross-chain collaborations.

Increasing Ecosystem Impact

Input Output (IOHK) enhances the impact of the Cardano community through a variety of strategic initiatives and support mechanisms:

- **Education & Training**: IOR supports the ecosystem through educational initiatives like open-access research, technical workshops, and tools such as Marlowe and Plutus, equipping the community with the knowledge to build and innovate.

- **Project Catalyst**: This community-driven innovation fund empowers users to propose, vote on, and fund new projects. It fosters a democratic approach to development and strengthens community ownership.

- **Strategic Partnerships**: IOR collaborates with academic institutions, industry leaders, and other blockchain initiatives to drive adoption, unlock new use cases, and expand Cardano's global reach.

- **Community Support**: By providing resources, funding, and infrastructure, IOR nurtures a thriving ecosystem that encourages innovation, inclusivity, and long-term sustainability.

1.11 Ethics

Ethics and research integrity are essential foundations for research excellence. They ensure that all academic activities are conducted with honesty, transparency, and respect for societal impact. Upholding these principles fosters trust, drives meaningful knowledge creation, and supports innovations that benefit Cardano's global community.

- **Commitment to Integrity and Transparency:** IOR's ethics policy is grounded in a strong commitment to integrity and transparency. All research must be conducted with honesty, rigor, and clarity, with findings accurately reported and openly shared. Researchers are expected to disclose any potential conflicts of interest and adhere to the highest standards of academic and scientific conduct. Transparent processes and outcomes are essential to maintaining trust within the community and with stakeholders.

- **Respect for Privacy and Data Security:** IOR is committed to safeguarding the privacy and data of all research participants. Data must be handled responsibly and in full compliance with applicable laws and regulations. Informed consent is required, with clear communication on the research purpose, data usage, and privacy safeguards. Anonymity and confidentiality must be preserved unless explicitly waived by participants.

- **Ethical Use of Technology:** IOR ensures that all blockchain technologies it develops or investigates are guided by ethical principles. Research should promote social good, minimize harm, and consider inclusivity, accessibility, and unintended consequences. Ethical risks must be identified and addressed before implementation.

- **Collaboration and Inclusivity:** IOR actively fosters collaboration and inclusivity by engaging a diverse range of stakeholders, including underrepresented groups. This ensures equitable outcomes, promotes diverse perspectives, and helps avoid disproportionate impacts on any community.

- **Accountability and Continuous Improvement:** IOR emphasizes accountability and the ongoing refinement of its ethical practices. Researchers are responsible for upholding standards and addressing ethical concerns. The ethics policy is regularly reviewed and updated to reflect technological advancements, evolving norms, and community feedback.

2. Cardano Vision

2.1 Introduction

To maintain its leadership in blockchain, Cardano requires a robust five-year Strategic Research Agenda focused on sustainability, scalability, and interoperability. Building on its track record of 100% uptime, the agenda aims to drive continuous technical advancement and ensure Cardano remains at the forefront of blockchain innovation. At its core, this vision sees Cardano—and the broader blockchain ecosystem—evolving into a decentralized compute and storage platform: a "world's operating system" where blockchains interoperate seamlessly, much like the frictionless connectivity we now take for granted in Web2.

This vision underpins the emergence of digital nation-states, where blockchain technology redefines identity, governance, and systems of power. To support this future, Cardano's research agenda outlines targeted R&D pathways that address foundational technical challenges and translate into real-world improvements across the protocol. The funnel-shaped approach generates impact on multiple fronts—expanding Cardano's presence in the global research community and producing tangible outputs such as peer-reviewed publications, technical specifications, and validated prototypes. Deep technologies like Web3 cannot rely solely on market demand; scientific and technical excellence requires early, sustained investment. By identifying and advancing high-potential areas now, Cardano accelerates innovation, secures long-term competitive advantage, and maximizes economic, societal, and environmental benefits.

2.2 Cardano Eras

Unlike other blockchains, Cardano does not rely on technical foundations taken from Bitcoin or other cryptocurrency systems. Instead, Cardano has adopted a research-led approach where IOR works with world-leading academics to address the fundamental research challenges necessary for creating a successful blockchain platform. Published research undergoes rigorous academic peer review, with papers presented at leading international conferences. This commitment to research helps determine what is possible and the most effective methods for achieving a successful outcome.

The technology that has been integrated into Cardano has been meticulously researched then specified by IOR and the broader research community which it engages. Peer review allows ideas to be critically evaluated and refined before implementation. This allows us to carefully consider multiple variables, including those often overlooked, to ensure the integrity and sustainability required for a global, decentralized platform. This is demonstrated in the papers and specifications that IOR has produced for each era of the Cardano Roadmap.

Byron

A period dedicated to building a foundational federated network that enabled the purchase and sale of ada. The first incarnation of Cardano allowed users to buy and sell the ada cryptocurrency on a federated network running the groundbreaking Ouroboros consensus protocol. The heart of the Cardano network, Ouroboros is the first proof-of-stake protocol created on the basis of academic research, with a

mathematically-proven level of security. As much as the Byron era was about the first crucial technology developments, it was also about building a community and getting people involved in creating the blockchain of the future

Papers

- Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol
- Ouroboros-BFT: A Simple Byzantine Fault Tolerant Consensus Protocol

Specifications

- A Formal Specification of the Cardano Ledger
- Specification of the Blockchain Layer
- Formal Specification for a Cardano Wallet
- Small Step Semantics for Cardano

Shelley

Shelley was designed to achieve a smooth, low-risk transition without service interruptions. A period of growth and development occurred for the network, focusing on ensuring greater decentralization. This phase led to enhanced security and a more robust environment, following the transition where the majority of nodes became operated by network participants.

Shelley also saw the introduction of a delegation and incentives scheme, a reward system to drive stake pools and community adoption. Painstakingly designed using game theory and the latest research into proof-of-stake networks, the delegation and incentive scheme allows and encourages users to delegate their stake to stake pools – always-on, community-run network nodes – and be rewarded for honest participation in the network.

Papers

- Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain
- Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability
- Stake-Bleeding Attacks on Proof-of-Stake Blockchains
- Reward Sharing Schemes for Stake Pools
- Account Management in Proof of Stake Ledgers
- Flexible Formality: Practical Experience with Agile Formal Methods
- Coalition-Safe Equilibria with Virtual Payoffs

Specifications

- Engineering Design Specification for Delegation and Incentives in Cardano–Shelley
- A Specification of the Non-Integral Calculations in the Shelley Ledger

Goguen

Where the Shelley era decentralized the core of the system, Goguen added the ability to build decentralized applications (DApps) on Cardano's solid foundation of peer-reviewed research and high-assurance development. The Goguen era introduced smart-contract functionality, enabling the construction of decentralized applications while supporting multifunctional assets, fungible, and non-fungible token standards.

One of the goals for the Goguen era has been the creation of Plutus, a purpose-built smart contract development language and execution platform using the functional programming language Haskell. The Goguen era also encompasses work to make Cardano accessible to wider audiences via Marlowe, a high-level, domain-specific language (DSL) for financial contracts which is built on Plutus. The Goguen era represented a step change in the abilities of Cardano, opening the way to the development of enterprise-level, mission-critical, decentralized smart contract applications,

Papers

- The Extended UTXO Model
- UTXOma: UTXO with Multi-Asset Support
- Native Custom Tokens in the Extended UTXO Model
- Functional Blockchain Contracts
- Scripting Smart Contracts for Distributed Ledger Technology
- Marlowe: financial contracts on blockchain
- Marlowe: implementing and analyzing financial contracts on blockchain
- Unraveling recursion: compiling an IR with recursion to System F
- System F in Agda, for fun and profit
- Translation Certification for Smart Contracts

Specifications

- A Formal Specification of the Cardano Ledger with a Native Multi-Asset Implementation
- A Formal Specification of the Cardano Ledger integrating Plutus Core

Basho

Basho is about improving the underlying performance of the Cardano network to better support growth and adoption for applications with high transaction volume. One of the core developments of Basho was the introduction of sidechains: new blockchains, interoperable with the main Cardano chain, with immense potential to extend the capabilities of the network.

Basho also saw the introduction of parallel accounting styles. While the main Cardano blockchain will continue to use an extended UTXO model, the ability to support and switch between UTXO and account-based models will be added using sidechains and layer 2 systems. The Basho era provides a

network infrastructure with the capability to scale in a sustainable, secure way, as well as the ability to add new functionality without compromising the reliability at the core of the network.

Papers

- Proof-of-Stake Sidechains
- Hydra: Fast Isomorphic State Channels
- Interhead Hydra: Two Heads are Better than One
- Mithril: Stake-based Threshold Multisignatures
- Babel Fees via Limited Liabilities
- Djed: A Formally Verified Crypto-Backed Pegged Algorithmic Stablecoin

Specifications

- Formal Specification of the Cardano Ledger for the Babbage era

Voltaire

The Voltaire era of Cardano will provide the final pieces required for the Cardano network to become a self-sustaining system. With the introduction of a voting and treasury system, network participants will be able to use their stake and voting rights to influence the future development of the network.

The development era is currently enabling the Cardano network to become a self-sustaining system. The Voltaire era will add the ability for network participants to present Cardano improvement proposals that can be voted on by stakeholders, leveraging the already existing staking and delegation process.

Papers

- A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence
- Updatable Blockchains
- SoK: Blockchain Governance

Specifications

- CIP-1694: An On-Chain Decentralized Governance Mechanism for Voltaire

2.2 Case Study: Ouroboros

First implemented in 2017 with Ouroboros (Classic), the Ouroboros consensus protocol marked a major milestone in distributed ledger innovation, particularly within proof-of-stake (PoS) systems. Developed for the Cardano blockchain, Ouroboros governs how the network reaches consensus, validates blocks, verifies signatures, manages token ownership, and determines the authoritative version of the blockchain.

Ouroboros also underpins Cardano's reward-sharing scheme, which incentivizes participation by allowing stakeholders to either operate a stake pool or delegate their stake. This inclusive model ensures broad participation in block production, driven by robust economic incentives.

A key innovation of Ouroboros is its use of provably secure, unbiased randomness in leader selection—offering strong security guarantees unmatched by many other protocols. Over time, successive iterations have built upon the original design, further strengthening the protocol's performance, scalability, and resilience.

Ouroboros Byzantine Fault Tolerance (BFT) enabled synchronized communication between a network of federated servers, preparing Cardano for the decentralized Shelley release.

Ouroboros Praos enhanced security and scalability, introducing private-leader selection and forward-secure, key-evolving signatures to protect against adaptive attaches and ensure block production

Ouroboros Genesis added a chain selection rule, allowing parties to bootstrap from the origin/genesis block without trusted checkpoints. Genesis evidences the protocol's Universal Composability with other protocols without losing its security properties.

Ouroboros Crypsinous builds on Genesis, adding the industry-first formally analyzed privacy-preserving proof-of-stake blockchain protocol feature, achieving security against adaptive attacks by introducing a new coin evolution technique relying on SNARKs and key-private forward-secure encryption.

Ouroboros Chronos introduces clock synchronization securely via a novel time synchronization mechanism and provides a cryptographically secure source of time to other protocols. Chronos makes the ledger more resilient to time based attacks.

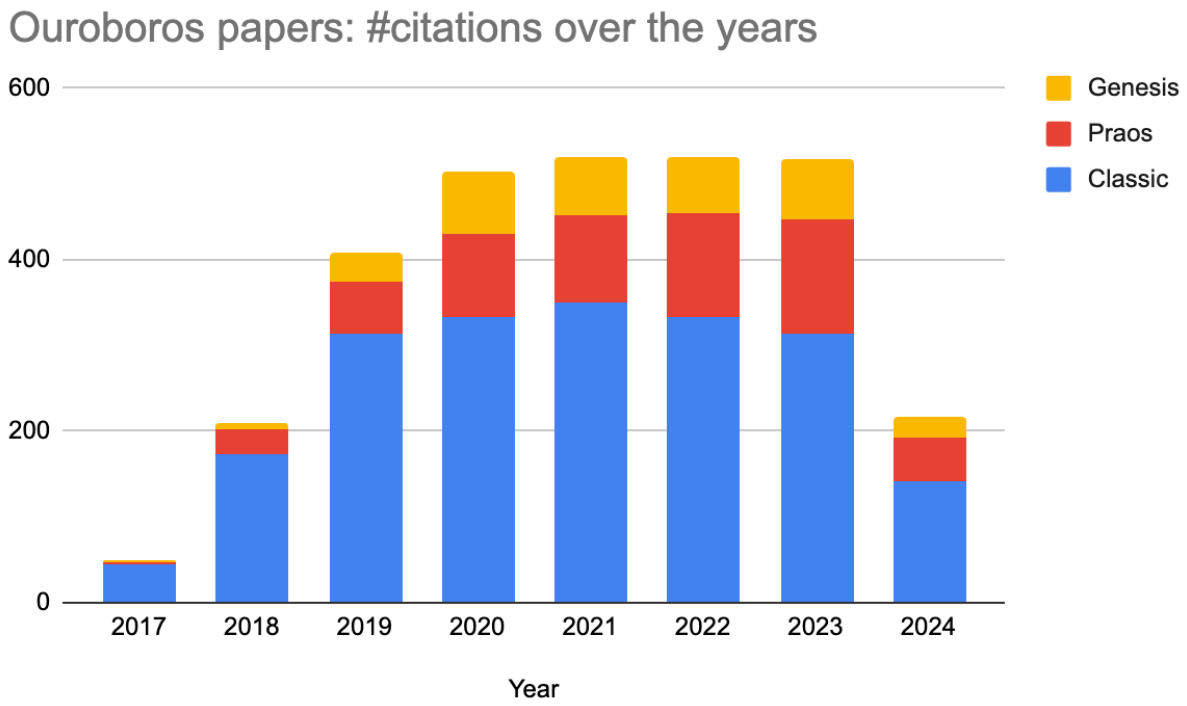

Figure 3: Ouroboros paper citations since 2017

The Ouroboros protocols are the result of rigorous, peer-reviewed research. All papers and supporting documentation are open-source, patent-free, and publicly available—published in leading cybersecurity and cryptography venues. This open approach ensures transparency and invites scrutiny, enabling anyone with the technical expertise to evaluate and challenge the protocol's claims.

To date, the Ouroboros papers—including Classic, Praos, and Genesis—have been cited nearly 3,000 times (see above) and adopted not only by Cardano but also by other blockchain platforms such as Polkadot, Mina, Horizen, and Concordium, which use derivatives of the protocol. This broad adoption underscores Ouroboros's influence and credibility within the blockchain research and development community.

2.3 Phased Timeline

As with all research tackling fundamental scientific questions, it is challenging to precisely estimate the timeline for completing each thematic focus area.

However, based on the deep expertise of the IOR team and its proven track record, we are confident that within 1–2 years, the team will deliver meaningful progress and propose to the Cardano community a portfolio of concrete improvements—or viable alternative options—ready for integration into the Cardano platform, based on the R&D outlined above.

To ensure alignment with evolving priorities, we propose a mid-term review after 2.5 years. This will follow the end of year 2026 report, take place during the 2027 work plan, and precede IOR's 2028 proposal.

The review will involve a three-month consultation process with Intersect and broader Cardano stakeholders to assess progress, identify challenges, and refine the vision for Cardano. This ensures the research remains aligned with industry innovation and Cardano's long-term goals, enabling continued leadership in blockchain R&D and adoption.

Phase 1: Breadth

In this first phase, multiple research directions are pursued to explore diverse solutions. Proposals are shared with engineering teams for implementation feedback, and with the wider Cardano community as the primary R&D stakeholder. Some paths may result in dead ends or yield sub-optimal outcomes, while others lead to impactful proposals. Each is thoroughly documented for community evaluation. Once the most promising directions are identified and accepted, the focus shifts to implementation planning.

Phase 2: Depth

Over the following 2–3 years, IOR will finalize peer review processes and deliver supporting artifacts in parallel with engineering development. This includes deeper R&D to formalize selected proposals, define parameterization, model security, and produce accompanying deliverables such as research papers, prototypes, and formal specifications. These outputs will not only inform Cardano's technical evolution but also provide the broader blockchain community with reusable insights, evidence, and a foundation for continued innovation.

2.4 Thematic Focus Areas

IOR's vision for Cardano ensures it can meet—and exceed—the evolving aspirations of the blockchain industry. Grounded in thorough impact assessments, five years of operational experience, and extensive consultation with stakeholders, this vision identifies nine thematic focus areas to guide Cardano's next phase of development. Each area addresses a core challenge or opportunity, supporting Cardano's evolution into a high-performance, globally relevant blockchain platform. Within each focus area, we outline the motivation, technical challenges, and expected benefits to Cardano. These include enhancements to interoperability, usability, performance, scalability, security, and developer utility—all crucial for supporting the builders who drive the ecosystem forward.

Other key themes include *identity, governance*, and *democracy,* by extending smart contract capabilities with identity-linked data; *consensus*, as the heart of the network evolves to meet demands for performance and reliability; and *tokenomics*, ensuring the right economic incentives are in place for participation and value creation. The agenda also includes *scalability*, through advanced Layer 2 protocols; *zero-knowledge proofs*, by standardizing a core technical architecture for ZK use cases; and *security*, with a strong emphasis on resilience in the face of growing threats, especially in a post-quantum world.

Together, these focus areas form a strategic roadmap to position Cardano as a foundational layer of the future internet—a world's operating system capable of supporting massive compute, data, and economic infrastructure. By concentrating resources on these priorities, Cardano ensures that its research is both visionary and grounded in practical outcomes that serve the long-term goals of the ecosystem.

(i) World's Operating System

Through blockchain-enabled digital assets, applications can not only transfer value but also define more complex instruments and interactions, such as those found in decentralized finance (DeFi).

To fulfill this vision, a blockchain platform must offer robust smart contract capabilities — supporting secure programming practices and providing the features developers need to build and deploy meaningful applications.

To position Cardano as a general-purpose operating system for decentralized applications, we identify seven key R&D directions that will guide its evolution and support this strategic goal.

WOS-1: Domain-specific languages for high-value applications (T3)

Domain-specific Languages (DSLs) enable domain experts to implement smart contracts and decentralized applications within their domain of expertise without the need for full-scale software development, thus significantly lowering the barrier to entry. Within Cardano, we have already demonstrated the feasibility and utility of this approach by developing, implementing, and launching the Marlowe DSL for financial contracts [WOS-1.1]. Building on this previous work, we propose to investigate other domains to find suitable candidates for DSLs for other high-value applications, such as legal applications, asset tokenization, and supply chain management.

Research goal: To develop the foundation for suitable DSLs in the style of Marlowe in three further domains.

Applications: Depending on demand from the community, three DSL environments in the style of the Marlowe implementation for Cardano.

Previous work: This project builds on IOR's previous work on Marlowe [WOS-1.1].

References: [WOS-1.1] Marlowe: implementing and analysing financial contracts on blockchain (Lamela et al., 2020)

WOS-2: State-machine contract environment (T3)

As part of the work on the various flavours of Hydra protocols, we observed that we can greatly simplify the development of smart contracts for Cardano by utilising a state-machine-based abstraction that hides many of the intricacies of the EUTxO model [WOS-2.1] [WOS-2.2] and provides a more declarative notion of smart contracts. This has led to the development of a formal framework tentatively called EasySM that takes care of all recurring mechanisms required for state-machine-based contracts on EUTxO. The goal of this research is to develop EasySM into an application programming framework for Cardano smart contracts.

Research goal: The goal of this research thread is to develop EasySM into an application programming framework for Cardano smart contracts and to define a formal semantics of that application programming

framework to facilitate the formal and mechanised reasoning about contracts implemented with that framework.WO2-1.

Applications: Hydra and DApp developers

Previous work: The papers [WOS-2.1], [WOS-2.2] introducing the EUTxO model defined a notion of state machines, CEMs, to express smart contracts and their relationship to transactions on the EUTxO ledger. The work on EasySM proposed here can be seen as a continuation of that previous work.

References [WOS-2.1] The Extended UTxO Model (Chakravarty et al., 2020), [WOS-2.2] Native Custom Tokens in the Extended UTXO Model (Chakravarty et al., 2020)

WOS-3: Formal verification of smart contracts (T3)

Smart contracts frequently lock assets of substantial value. Hence, to avoid financial loss, it is crucial to assess the correctness of such contracts and the tools used to generate and execute contract code. In Cardano, we have a solid foundation due to the use of formal methods in the development of Plutus smart contracts. Moreover, we have made substantial progress in establishing methods for the formal reasoning about the correctness of the compilation of contract code.

Research goal: This research aims to develop a formal verification methodology for smart contracts using state machines. By reasoning directly about the contract's source code, we will establish functional correctness, security, and liveness properties. The approach builds on the formal semantics of EasySM, enabling verification within Agda.

Applications: Any smart contract developed with EasySM can be used as an application. This includes the EasySM contracts developed as part of Hydra.

Previous work: This proposal leverages work done on EasySM to date, as well as the forthcoming effort to formalise the semantics of EasySM in Agda outlined in the "State-Machine Contract Environment" stream.

References: [WOS-3.1] Hydra: Fast Isomorphic State Channels (Chakravarty et al., 2021)

WOS-4: Decentralized storage (T2, T6, T7)

Decentralized storage marks a shift from traditional centralized data storage, where a single entity or a network of central servers manages data. In decentralized systems, data is spread across multiple nodes in a peer-to-peer network, enhancing security and resilience by eliminating single points of failure. However, in permissionless environments typical of blockchain technology, where anyone can join without authorization, the design of these systems must account for corrupted nodes. These potentially malicious participants can deviate from prescribed protocols, posing risks to the system's integrity, security, and functionality.

Research goal: This research focuses on developing decentralized storage solutions resilient to Byzantine failures. While Distributed Hash Tables (DHTs) show promise, current designs rely heavily on

heuristics. The goal is to create a provably secure protocol—whether by leveraging DHTs or introducing a novel alternative.

Applications: A Byzantine-resilient storage layer can extend smart contract capabilities beyond UTXOs, securely store NFT-linked files, and serve as a robust persistence layer for pub/sub systems—enhancing security, decentralization, and efficiency across use cases.

Previous work: IPFS [WOS-4.1] offers a peer-to-peer network for storing and accessing files, websites, applications, and data, while Filecoin is a decentralized storage network built on blockchain that incentivizes users for storing data. Furthermore, concepts like proof of storage [WOS-4.3], replication [WOS-4.4], and retrievability [WOS-4.5] play a crucial role in ensuring the integrity and accessibility of data in decentralized environments. These foundational works and concepts form the backdrop against which this research seeks to innovate, aiming to contribute a novel, secure, and efficient solution to the challenges of decentralized storage in the blockchain era.

References: [WOS-4.1] The InterPlanetary File System (IPFS), [WOS-4.2] Filecoin, [WOS-4.3] Provable Data Possession at Untrusted Stores (Ateniese et al., 2007), [WOS-4.4] Tight Proofs of Space and Replication (Fisch et al., 2018), [WOS-4.5] Pors: proofs of retrievability for large files (Juels et al., 2007)

WOS-5: Pub/sub communications (T3)

A robust communication framework is essential for any decentralized ecosystem to enable seamless interaction and information exchange. Currently, Cardano lacks a systematic approach to several critical communication needs. There are no efficient mechanisms for DApps to interact with one another, and observing smart contract activity often requires monitoring the entire blockchain state—a highly resource-intensive process. Moreover, there is no standard method for stake pool operators (SPOs) to communicate important updates to their stakeholders.

Research goal: This proposal aims to develop a secure, innovative publish-subscribe (pub/sub) system with provable resilience to Byzantine faults, ensuring reliable communication between publishers and subscribers in decentralized networks.

Applications: This system enables efficient communication between dApps, smart contracts, and SPOs without full blockchain monitoring, addressing key communication gaps and strengthening the overall reliability of the decentralized ecosystem.

Previous Work / References: n/a

WOS-6: Location-based services and smart contracts (T3)

This workstream explores how geographic location can influence blockchain state transitions and smart contract behavior—enabling use cases like location-based payments, region-specific DeFi rules, and automated billing via physical infrastructure access. It also examines the critical role of node location in enhancing network resilience, as greater geographic diversity can reduce the risks of geopolitical interference, natural disasters, and eclipse attacks. Key research questions include how to accurately measure geographic diversity using Internet topology, and how to design incentives that encourage globally distributed node placement.

Research goal: (1) Develop and design secure location-based smart contracts (2) How to incentivize, reward and enforce geographic diversity among the consensus nodes

Applications: (1) Novel location-based services (2) reward/enforcement of geographic locations of consensus nodes. As a first step, Cardano would commission a localization protocol that verifies SPOs' locations and uses the output in a modified reward scheme with an additional geographic component.

Previous Work / References: [WOS-6.1] VerLoc: Verifiable Localization in Decentralized Systems (Kohls, et al, 2022)

WOS-7: Intent-based ledgers and decision making (T3,T7)

In blockchain systems, *intents* represent user-defined goals for updating the ledger state. On Cardano, limited intent functionality is currently achievable through a mix of smart contracts and off-chain coordination, often requiring complex co-construction of transactions between multiple users. However, insights from the development of the Babel fees mechanism [WOS-7.1] revealed that certain use cases—such as atomic swaps—could be enabled more efficiently by making targeted changes to the ledger, eliminating the need for smart contracts or direct user communication. This workstream explores extending that approach to support a broader range of intents, enabling faster, cheaper, and more seamless interactions that are currently difficult or impractical to implement.

Research goal: This research aims to develop a general framework for processing *intents* [WOS-7.3]—transactions that require additional data from other transactions to complete—by replacing individual transactions with *validation zones* as the atomic units of validation. Each zone contains a list of partially valid transactions, and is only considered valid when all intents within it are fulfilled, enabling more flexible and efficient ledger updates.

Applications: Three potential applications have emerged for this framework: Babel fees (using validation zones) [WOS-7.1], ledger support for a potential light client protocol [2], and data sharing—enabling temporary storage accessible by multiple transactions within a zone.

Previous Work: The CIP [WOS-7.2] formalizes specific kinds of intents (babel fees and others), and the CPS [WOS-7.4] describes the idea of intents in more detail.

References: [WOS-7.1] Babel fees via limited liabilities (Chakravarty et al., 2022), [WOS-7.2] Nested Transactions (P. Vinogradova), [WOS-7.3] Intents on Cardano (M. P. Jones), [WOS-7.4] Agda formalization, [WOS-7.5] Native Custom Tokens in the Extended UTXO Model (Chakravarty et al., 2020)

(ii) Ouroboros Omega

Cardano uses the Ouroboros protocol as its underlying consensus layer. Ouroboros enables energy-efficient proof-of-stake operation and an unbounded number of active participants following a blockchain discipline akin to Nakamoto's longest chain protocol logic. There are still many ways in which the Ouroboros protocol can be improved to accommodate the demand for transaction throughput and processing that will come as the Cardano ecosystem expands.

We present below the seven different R&D directions that we identify as critical to be pursued to evolve the protocol to its final form, Ouroboros “Omega”, the final letter in the Greek alphabet.

OO-1: Ouroboros Peras - Vision (T1)

Cardano currently uses Ouroboros Peras, a longest-chain proof-of-stake protocol known for its robustness and resilience to fluctuating participation and adversarial conditions. However, its gradual settlement—requiring many blocks to achieve finality with high assurance—can hinder adoption and complicate certain layer 2 deployments. Ouroboros Peras addresses this limitation by significantly improving settlement times. A first version has been delivered, demonstrating promising gains. Further research is needed to fine-tune parameters and enhance resilience—particularly in avoiding cooldown phases, a non-trivial challenge that, once addressed, will make Peras even more effective.

Research goal: To enable fast settlement in the Ouroboros protocol family under typical conditions—high participation and low adversarial activity—while maintaining existing robustness, and falling back to current settlement speeds under less favorable conditions such as low participation, network hiccups or an adversarial attack.

Applications: The primary application is for the Cardano mainchain, though the resulting protocol could also benefit future systems using longest-chain consensus protocols.

Previous Work: A first version of the protocol has been published and formally validated, demonstrating promising gains.

References: A first paper on boosting settlement times in Cardano is expected Q2 2025, with improvements to the protocol investigated afterwards.

OO-2: Ouroboros Leios (T1)

Praos, the current Ouroboros protocol, is nearing its throughput limits, constrained by block size and timing. It underutilizes available network resources like bandwidth, CPU, and memory. Leios addresses this by enabling throughput that scales with node capacity—doubling a node’s resources results in roughly double the throughput. This vertical scalability is essential to meet the demands of a growing ecosystem of blockchains and sidechains. Leios aims to be the first Ouroboros protocol where performance directly reflects the resources of participating nodes.

Research goal: To formally specify the next generation of Ouroboros that optimally uses the network bandwidth to solve the scalability issues of Cardano on L1. The proposed algorithm must be proved secure in the standard security model of Cardano and subsequently equipped with a proper incentive model.

Applications: The primary application is to increase Cardano’s throughput to support the growing demands of new service chains and smart contracts, by better utilizing underused network CPU capacity—currently below 15% (currently CPU’s of SPOs are used for less than 3 seconds every 20 seconds to validate block content/smart contracts).

Previous Work: While many papers claim throughput optimality, few substantiate these claims within a rigorous security model. The most notable work on security in bounded bandwidth settings is [OO-2.1], which analyzes PoW/PoS Nakamoto Consensus but does not address throughput. Related works, such as [OO-2.2] , also claim optimality, but rely on overly idealized models. A separate line of research beginning with Narwhal [OO-2.3] introduces a committee-based protocol for asynchronous networks, tolerating up to one-third corrupt parties, and also claims throughput optimality—yet lacks formal proof and is limited to the permissioned setting.

References: [OO-2.1] Security of Nakamoto Consensus under Congestion (Kiffer et al., 2024) [OO-2.2] Deconstructing the Blockchain to Approach Physical Limits (Bagaria et al., 2018), [OO-2.3] Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus (Danezis et al., 2022) [OO-2.4] High-Throughput Blockchain Consensus under Realistic Network Assumptions (Coretti-Drayton et al., 2024)

OO-3: Fair transaction processing (T8)

Like Bitcoin and Ethereum, Ouroboros currently offers no guarantees against front-running or preferential transaction ordering. This lack of fairness enables practices like Maximal Extractable Value (MEV), which can harm users and distort markets. Existing mitigations, such as proposer-builder separation, may reduce MEV but risk centralizing a layer 1. This stream develops protocol-level solutions to make fair transaction processing a default feature that benefits end users. It includes designing and implementing cryptographic techniques and consensus modifications to ensure equitable ordering without compromising decentralization or performance.

Research goal: A fair transaction processing layer for Ouroboros.

Applications: If successful, this research could become a unique selling point for Cardano, as no public blockchain currently offers fair transaction processing.

Previous Work / References: [OO-3.1] Universal Composable Transaction Serialization with Order Fairness (Ciampi et al., 2024), [OO-3.2] Ordering Transactions with Bounded Unfairness: Definitions, Complexity and Constructions (Kiayias et al., 2024)

OO-4: Byzantine-resilient networking (T6, T8)

In a blockchain protocol, the backbone that allows for seamless operation and robustness is its networking infrastructure. Consensus protocols have been studied extensively in the presence of a Byzantine adversary, showing how to maintain protocol integrity despite malicious actors. However, until recently, the narrow focus on consensus algorithms left the underlying gossip network susceptible to vulnerabilities. Research has demonstrated the construction of a Byzantine-resilient gossip layer and has shown the resilience of the Ouroboros Praos protocol when running on this newly secured network layer.

Research goal: This research aims to address key limitations in the protocol outlined in [OO-4.1], focusing on improving inclusivity, security, and practical applicability. It will extend the model to incorporate bandwidth constraints, examining data diffusion and synchronization challenges in high-throughput settings. The project also seeks to include low-stake SPOs, relays, and client nodes

without compromising Sybil resistance. Additionally, it will rigorously analyze and validate eclipse-resistance strategies to reduce vulnerability under real-world node connectivity limits. Finally, it aims to bridge theory and practice by formally assessing real-world DoS mitigation mechanisms.

Applications: This research aims to offer a more grounded and nuanced understanding of the network layer], bolstering confidence in its real-world application. The insights gained from this work are expected to provide a clearer theoretical perspective on certain critical mechanisms, leading to more reliable and practical network implementations. Another key aspect of this work is the development and analysis of a networking layer for the bandwidth-constrained setting, which holds particular relevance for the Leios project.

Previous Work: The above refers to the construction of a Byzantine-resilient gossip layer [OO-4.1] and the foundational work on security in bounded bandwidth settings by [OO.4-2].

References: [OO-4.1] The Generals' Scuttlebutt: Byzantine-Resilient Gossip Protocols (Coretti et al., 2022), [OO.4-2] Security of Nakamoto Consensus under Congestion (Kiffer et al., 2024)

OO-5: Multi-resource consensus - Minotaur (T4, T8)

Minotaur explores consensus mechanisms that combine multiple resources, like proof of work (PoW), proof of stake (PoS), and proof of restake (PoRS) to improve security and resilience. By using diverse inputs, the system can maintain integrity even if one resource is compromised. This is especially useful when bootstrapping new blockchains facing low liquidity or uneven stake distribution. Leveraging existing assets—such as restaked PoS—enables early-stage networks to draw on stable participants for secure operation. Minotaur supports flexible, hybrid consensus for more robust and inclusive decentralized systems.

Research goal: To explore multi-resource consensus from first principles, with an emphasis on BFT consensus and PartnerChains applications. This thread aims to formally define and prove how diverse resources—across chains or including proof-of-work and useful work—can be securely measured and combined into a single metric for block production, enabling resilient and inclusive consensus protocols.

Applications: Multi-resource consensus enables secure bootstrapping of PartnerChains by combining Cardano stake and SPOs with native tokens to power their base layer from the outset.

Previous Work: The Minotaur [OO-5.1] paper considered the special case of combining PoW and PoS into multi-resource consensus for Nakamoto-style blockchains.

References: [OO.51] Minotaur: Multi-Resource Consensus (Fitzi et al., 2022), [2] Proof-of-Stake Sidechains (Gaži et al., 2019)

OO-6: Proofs of useful work (T7)

This research integrates real-world computational tasks into blockchain consensus via PoUW. Unlike traditional PoW, which wastes energy, PoUW secures the network through valuable work such as solving SAT problems, generating zk-SNARKs, or training ML models. Building on the Ofelimos protocol—IOG's

first provably secure PoUW design—this research explores extending the concept to large-scale optimization and scientific computation. It enhances Cardano's security while offering a sustainable and accessible on-ramp for new participants contributing useful computation to the ecosystem.

Research goal: To explore Proofs-of-Useful-Work for securing blockchain protocols from first principles, addressing three core challenges: defining useful work, ensuring protocol security across diverse tasks, and identifying future-relevant task examples.

Applications: This research supports Minotaur by adding Proofs of Useful Work (PoUWs) as a resource in multi-resource consensus, boosting security with untapped computational power. PoUWs for SNARKs may also improve blockchain maintenance and enable faster validation for more efficient light nodes.

Previous Work: While numerous papers propose PoUW systems, only [1] and [2] include formal security analyses. [1] focuses on PoUWs for optimization via stochastic local search, while [2] targets PoUWs for SNARKs used in Bitcoin ledger correctness proofs. However, the PoUW in [2] is not generic and applies only to a specific SNARK statement tailored to that use case.

References: [OO-6.1] Ofelimos: Combinatorial Optimization via Proof-of-Useful-Work (Fitzi et al., 2022), [OO-6.2] Proof of Necessary Work: Succinct State Verification with Fairness Guarantees (Kattis et al., 2021)

OO-7: Congestion control (T1,T2)

This workstream rethinks blockchain fee models to manage congestion more effectively. Current flat or dynamic fees bundle all resource costs into one price, offering limited control or predictability. Users cannot express transaction urgency, making DeFi and high-priority use cases harder to support. Dynamic fees respond to demand but are unpredictable; flat fees are stable but vulnerable to spam. This research proposes a more nuanced system where fees reflect resource usage and urgency—enabling fairer, more efficient and attractive transaction processing under varying Cardano network conditions.

Research goal: This research aims to broaden congestion control mechanisms by improving application diversity (supporting varied use cases like DeFi and payment channels), predictability (enabling users to know transaction costs and delays in advance), and resource heterogeneity (pricing resources like bandwidth and storage differently). The approach builds on and extends Tiered Pricing [OO-7.1], which enhances EIP-1559 by offering service levels with trade-offs between wait time and cost.

Applications: The primary application is the Cardano transaction fee mechanism. Predictable service guarantees are crucial for business use cases, where budgeting often occurs well before transactions are created. Supporting application diversity fosters ecosystem growth by enabling a wider range of use cases, while addressing resource heterogeneity ensures optimal use of the network's varied resources.

Previous Work: While blockchain transaction fee mechanisms have been widely studied, no fundamentally superior design has yet emerged.

References: [OO.71] Tiered Mechanisms for Blockchain Transaction Fees (Kiayias et al., 2024), [OO-7.2] Designing Multidimensional Blockchain Fee Markets (Diamandis et al., 2023), [OO-7.3] Blockchain Space

Tokenization (Kiayias et al., 2024)

OO-8: Cardano sharding (T1)

Blockchain throughput and latency are constrained by how quickly a single node can download and validate data. Traditional protocols replicate the full ledger and validation process across all full nodes, leading to inefficiency as more nodes join. Sharding addresses this by enabling horizontal scaling—performance improves with more nodes—by assigning each node only a portion of the ledger to store and validate. This reduces individual node workload and enhances overall protocol throughput and latency.

Research goal: The goal is to research blockchain sharding from first principles, critically re-evaluating previous claims and designing a protocol that increases throughput as more nodes participate in block production, while preserving latency comparable to the underlying unsharded protocol.

Applications: Sharding has the potential to deliver full horizontal scaling for Cardano, offering performance improvements beyond those achieved by Leios and Hydra.

Previous Work / References: [OO-8.1] Selection of Schemes: Instachain, GearBox, RapidChain, PolyShard, [OO-8.2] Information Dispersal with Provable Retrievability for Rollups (Ozdayi et al., 2022), [OO-8.3] Efficient Cross-Shard Transaction Execution in Sharded Blockchains (Das et al. 2021), [OO-8.4] Free2Shard: Adaptive-adversary-resistant sharding via Dynamic Self Allocation (Rana et al., 2020), [OO-8.5] SoK: Sharding on Blockchain (Shi et al., 2019)

(iii) Tokenomicon

Tokenization is one of the fundamental innovations of blockchain technology. It enables blockchain users to define tokens that abstract different perspectives of real world value and facilitate value transfer seamlessly at a global scale.

Cardano is at the forefront of these innovations with its unique set of features, which include native user-defined assets, and upcoming innovations such as Babel fees, which facilitate transaction fees payable in arbitrary tokens.

Interestingly, despite being a fundamental feature of blockchain technology, tokenomics remains also one of the most under researched areas. Below we identify three relevant research directions that would be crucial to undertake for the Cardano ecosystem.

TO-1: Tokenomics design (T4)

This stream investigates first principles in tokenomics to inform long-term macroeconomic policies for the Cardano ecosystem. Sustaining token value is essential for security and user adoption. We will develop mathematical models to evaluate the system's ability to reach and maintain long-term equilibrium, reflecting Cardano's decentralized and diverse nature. These models will guide optimal token circulation and support evidence-based parameter choices for ecosystem stability—such as treasury, reserves, and

token supply adjustments.

Research goal: Identify the key parameters in the Cardano ecosystem that impact the token price evolution, and suggest optimal parameter choices and possible venues for improvement of the current design. To this end, we shall develop the necessary mathematical models that account for the heterogeneous and decentralized nature of the Cardano ecosystem.

Applications: Develop additional governance tools to empower the Cardano community to make informed, long-term decisions that support the platform's economic stability, resilience to external shocks, and capacity for innovation—such as strategic treasury management—while maintaining strong security guarantees.

Previous Work: Existing tokenomics models (see below) cannot capture the Cardano fundamental design components (reward sharing, transaction fees, treasury, reserve, etc).

References: [TO-1.1] Would Friedman Burn your Tokens? (Kiayias et al., 2023), [TO-1.2] Blockchain Platform Design under Market Frictions (Häfner, 2023)

- **Traditional Approaches (users' perspective only):** [TO-1.3] Tokenomics: Dynamic Adoption and Valuation (Cong et al., 2021), [TO-1.4] The Value of Decentralization Using the Blockchain (Reuter, 2022)
- **Competition & PoS security (validators' perspective only):** [TO-1.5] Competitive Equilibria Between Staking and On-chain Lending (Chitra, 2021),
- **(Post) Modern portfolio theory and cryptocurrencies:** [TO-1.6] Risk-Based Portfolio Optimization in the Cryptocurrency World (Burggraff, 2019), [TO-1.7] Time frequency analysis of the commonalities between Bitcoin and major Cryptocurrencies: Portfolio risk management implications (Mensi et al., 2019)
- **Dual-token Systems (no equilibrium / no prices analysis):** [TO-1.8] The Economic Value of Dual-Token Blockchains (Dimitri, 2023), Dual-token Systems (equilibrium & prices analysis, advantages over single-token), [TO-1.9] Single-token vs Two-token Blockchain Tokenomics (Kiayias et al., 2024)
- **Restaking Models:** [TO-1.10] Robust Restaking Networks. (Durvasula and Roughgarden, 2024) [TO-1.11] How much should you pay for restaking security? (Chitra and Pai, 2024)

TO-2: Rewards sharing and transaction fees (T4)

A key factor in enabling successful decentralized blockchain operation is properly incentivizing participants. This is primarily achieved through well-designed reward schemes that distribute revenues from block production and transaction fees to encourage desirable behavior. However, designing these schemes is complex. Challenges include maintaining anonymity, addressing player asymmetries (e.g., between stake pool operators and delegators), and ensuring decentralized implementation. While more sophisticated reward mechanisms have emerged in recent years, there remains significant room for improvement and this workstream aims to achieve more robust, fair, and efficient reward distribution whilst ensuring Cardano is an attractive service platform for end users with fair fees.

Research goal: This research aims to conduct an in-depth analysis of reward sharing schemes using game-theoretic methods, with the goal of designing improved mechanisms that enhance decentralization

and inclusivity. Practically, it will provide concrete suggestions for refining Cardano's current reward system, while also informing related components such as DRep rewards in Voltaire and potential reward models for Mithril certification.

Applications: The main application will be the Cardano reward sharing scheme that is being used for distributing rewards from block production and transaction fees to SPOs and their pool members. Furthermore, ideas developed under this stream could be applicable for all other reward schemes within Cardano, such as the dRep rewards for governance actions, which is currently under design, the rewards for reviewers and delegates in Project Catalyst, and potential rewards for Mithril certification.

Previous Work / References: [TO-2.1] Reward Sharing Schemes for Stake Pools (Brunjes et al., 2020), [TO-2.2] Decentralization Analysis of Pooling Behavior in Cardano Proof of Stake (Ovezik and Kiayias, 2022)

TO-3: Stablecoins (T6)

Stablecoins have become an indispensable part of the cryptocurrency economy and are catalytic to the wider use and adoption of any blockchain platform. Their uses are multiple such as providing liquidity, facilitating trading and DeFi, offering an on-chain store of value with low volatility, and more. A variety of designs have been put forth so far, with very different mechanics to achieve stability. These include the collateralized stablecoins (either with crypto tokens or fiat currency), algorithmic designs that maintain the peg by careful regulation of supply and demand and many other hybrid approaches. Crucially, they all attempt to solve the same underlying issue, exchanging the risk (and reward) of a volatile asset for price stability, at a cost. There is no optimal solution, as any solution faces a fundamental trade-off between centralization, price stability, capital efficiency and cost, which can only be attractive to specific users, based on their beliefs, risk preferences and use cases. Finally, regulatory compliance is stricter for stablecoins and extra care needs to be taken if they are to be widely adopted.

Research goal: This research has two main objectives: first, to better understand the risks of maintaining stablecoins—particularly non-fiat-backed—where de-pegging can result from asset decline or coordination failures akin to bank runs. Second, by identifying which designs and parameters best mitigate these risks, we aim to develop a unified theory of stablecoin design trade-offs to guide the creation or improvement of robust, optimal stablecoins.

Applications: Expand the Cardano stablecoin ecosystem by enhancing Djed and introducing additional designs tailored to diverse use cases and risk preferences.

Previous Work: There is significant work in risk management from finance and the Diamond-Dybvig model for bank runs. However, neither are immediately amenable to the unique challenges of a decentralized stablecoin.

References: n/a

(iv) Global Identity

Decentralized identity has been in the works for some time, promising to power the next generation of digital identity services. Decentralized identity will shift control to end users (Self-sovereign identity), without sacrificing usability or security, as well as enabling advanced features such as decentralized reputation management and, along the way, potentially new notions of what an *identity* is. Moreover, they are designed and specified in a standards-like fashion, with the aim of ensuring interoperability.

GI-1: Decentralized identity and reputation management (T8, T9, T10)

This workstream explores the design of a global identity system that gives Cardano users full control over their digital identities across platforms, allowing selective sharing of personal information. It focuses on defining a general, implementation-independent framework built on formal abstractions of trusted components like credential systems and public key infrastructures. The goal is to identify trade-offs between different design choices and develop practical, efficient implementations. The work also examines how identity systems interact with applications, including cross-platform identity portability, and how to integrate these systems into the broader digital identity landscape.

Research goal: Although no formal definition of a global identity exists, terms like “decentralized,” “privacy-preserving,” “user-centric,” and “self-sovereign” frequently appear in digital identity discussions. This research aims to define the foundations of a global identity system, connect it to current and emerging trends—such as decentralized identifiers, verifiable credentials, and anonymous credentials—and explore how to integrate these concepts natively within the Cardano ecosystem. A key focus will be understanding Cardano’s role as a potential backbone for this evolving identity framework.

Applications: To integrate the notion of global identity (or, rather, an instantiation of it) within Cardano’s core (transactions, smart contracts, governance) and the wider Cardano ecosystem. Additional applications include augmenting existing stacks to be compatible with this notion of global identity.

Previous Work: The formalization of DIDs which is directly connected with the first steps of this research thread. Additionally, we have defined the notion of “Universal Anonymous Signatures” [GI-1.1], which sets the foundation of what could be one of the pillars to achieve a global identity notion. [GI-1.2] We have also formally analyzed relevant auxiliary protocols in the space, such as DIDComm (for establishing secure communication channels using DIDs), which is likely to be useful when aiming at integrating our notion of a global identity into existing stacks.

References: [GI-1.1] Foundations of Anonymous Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions (Bobolz et al., 2024), [GI-1.2] What DIDComm Out of It? Analysis and Improvements of DIDComm Messaging (Badertscher et al., 2024**)**

(v) Democracy 4.0

Manville and Ober in their ‘In search of Democracy 4.0’ article [8], divide the history of democracy in three distinct phases, highlighting that even though it significantly evolved over time, it did maintain its essential core. Democracy 1.0 points to paleolithic political systems where small foraging communities got together

and engaged in decision making led by elders or others whose role was mostly situational. Democracy 2.0 is reflected in ancient Athens and other similar city states. It illustrates some more extensive use of basic technology in decision making that includes written registries, lottery machines for randomized appointments, and vote recording methods.

Finally, Democracy 3.0 points to post-enlightenment Europe, with its large-scale inclusivity and representation reflected in modern democracies as practiced in the USA, India, European Union, and others. Use of technology has gradually become more extensive, with digital tabulation and transmission of partial results across large geographic areas, and even digital recording of votes in some cases. At present, the advent of the internet, social media, and artificial intelligence pose major challenges for the existing democratic processes. New technological advances also present opportunities for rethinking the democratic process while maintaining all its core principles and adapting it to the 21st century. This can lead us to Democracy 4.0.

D4-1: Next-level governance protocols (T8, T11)

This stream designs scalable, decentralized governance systems to ensure Cardano's long-term sustainability. While CIP-1694 meets current needs, it may not scale under future conditions like network congestion. We explore alternative voting models—stake-based, representative, and liquid democracy—that maintain broad, reliable participation. Most e-voting protocols rely on centralized tallying or are too costly for blockchain use. This work aims to develop low-footprint, secure, decentralized governance solutions that align with Cardano's Constitution, balancing off-chain and on-chain computation for efficient, transparent and future-proof deployment.

Research goal: The goal is to capture governance requirements for applications within the Cardano ecosystem and design a suite of robust, secure protocols that address those needs—balancing trade-offs around cost, scalability, runtime, and Layer 1/Layer 2 impact. A secondary objective is to extend these solutions to the broader Cardano ecosystem in a subsequent phase.

Applications: Application of this research lies in any blockchain governance application that requires participation of various blockchain stakeholders in the decision making process. It will also have relevance in scenarios where layer 2 protocols are being developed to off-load the cost of protocols running on the mainchain with large scale participation.

Previous Work: Prior research [D4-1.1] provides a framework for blockchain governance and voting using the blockchain itself.

References: [D4-11] A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence (Zhang et al., 2019), [D4-1.2] Mithril: Stake-based Threshold Multisignatures (Kiayias et al., 2024)

D4-2: Governance incentives (T8, T11)

While sufficient robustness has been achieved in respect to the alignment of participant goals of a blockchain ecosystem, it is difficult to balance swift and effective decision making with the fundamental blockchain principles of decentralization, security, transparency, and fairness. This is particularly challenging now that the set of blockchain participants has been expanded and cannot be adequately

captured just by the number of tokens owned by each wallet.This workstream aims to design the right incentive schemes for this complex governance landscape, starting with DReps before extending to all other participants.

Research goal: The primary objective is to investigate key research questions related to Voltaire and Project Catalyst, starting with the viability of alternative voting rules for governance actions—focusing on preventing centralization, ensuring Sybil resistance, and capturing voter preferences beyond the "1 token, 1 vote" model (e.g., Quadratic Voting and others). The research will then explore treasury fund allocation, aiming to balance budget constraints with proportional representation, avoiding scenarios where a simple majority dominates all decisions. Promising, recently proposed approaches will also be evaluated in this context.

Applications: Both Voltaire and Project Catalyst will benefit from the outcome of this research, which could produce novel more expressive and decentralized voting rules.

Previous Work: There is extensive research in social choice theory on voting rules. Below, we highlight a few key sources particularly relevant to quadratic voting, blockchain governance, and the Method of Equal Shares, which serve as a useful foundation for further exploration in this context.

References: [D4.2-1] A Flexible Design for Funding Public Goods (Buterin, Hitzig and Weyl, 2020), [D4-2.2] Proportional Participatory Budgeting with Additive Utilities (Peters, Pierczyński and Skowron), [D4-2.3] SoK: Blockchain Governance (Kiayias and Lazos, 2022)

D4-3: Decision-making toolset (T8, T11)

This research stream focuses on developing tools to support objective, accountable, and collaborative decision-making within the Cardano ecosystem. It aims to enable participants to assess and compare proposals across key dimensions such as decentralization, cost, utility, token value, interoperability, regulation, and throughput. Central to this is the creation of a performance modeling system for first-principles comparison of technical proposals. Building on efforts like the Edinburgh Decentralization Index (EDI) [12], similar methodologies will be applied to other metrics. Additionally, a subthread will explore decentralized infrastructure to support transparent, private, and accountable deliberation processes.

Research goal: To facilitate sound decision making and sustainable development, governance requires tools for metrics and assessment of both past decisions as well as current pain points and trends. To address this need, this research direction will develop tools that estimate various metrics of interest — similar approaches such as the one illustrated in EDI can be used to offer visualisations of how different systems operate and compare with each other when various relevant metrics of interest are considered. Part of the research is to determine exactly what needs to be measured, through first principles and community consultations, as well as develop methodologies that facilitate the measurements and develop and realize the required algorithms.

Applications: Voltaire as well as Project Catalyst will benefit from the outcome of this research, as it will enable the community to identify directions for improvement as well as enable historical comparisons stemming from previous decisions and the way they impacted metrics of interest.

Previous work: The Edinburgh Decentralization Index (EDI) is the most prominent current example of such a tool (still under development).

References: [D4.3-1] Measuring Blockchain Decentralization, (Ovezik, Karakostas, Milad, Kiayias, Woods, 2025).

(vi) The Internet Hydra-ted

Cardano, like other blockchain platforms, aspires to be a universal infrastructure capable of supporting any user-deployed application. To maintain broad accessibility, the platform is intentionally engineered to prioritize inclusivity over raw performance. However, this trade-off can limit the ability to run high-performance applications comparable to those in Web2 environments. Layer 2 protocols offer a solution, enabling scalability and responsiveness without compromising the underlying platform's inclusivity.

Within the Cardano ecosystem, Hydra serves as the core state-channel (SC) protocol suite designed to address these layer 2 scaling needs. SCs allow transactions to be executed off-chain, reducing the load on the main chain while maintaining trust assumptions—at least in optimistic scenarios with honest participation. This approach significantly improves throughput and latency, enabling faster and more efficient transaction processing.

Currently, only the Hydra Head protocol has been implemented. To fully realize Hydra's potential and unlock comprehensive layer 2 capabilities for Cardano, further research and development are required across several remaining components of the Hydra protocol suite.

IHT-1: Hydra Tail (T1)

Hydra Tail extends Cardano's layer 2 scaling via zk-rollups, complementing the Hydra Head protocol. It batches off-chain transactions and posts succinct proofs to layer 1, reducing on-chain load while ensuring security through zero-knowledge proofs. Users can move funds and contracts between chains with strong censorship resistance. The protocol follows a SC model—moving from an initial state to open, failed, or closed states depending on activity and disputes. A special registered transaction (regTx) allows clients to bypass censorship and safely reclaim funds if needed.

Research goal: The main goal of this research thread is to design and analyze a zk-rollup protocol from first principles through a provable security perspective. In particular we aim to (i) Define what functionalities a secure zk-rollup protocol should ideally provide (ii) Design and analyze a solution for UTxO-based ledgers that strikes a good balance between security, simplicity, and mainchain footprints.

Applications: Hydra Tail will enhance Cardano's set of scaling solutions, thus reducing transaction costs and attracting a larger user base.

Previous Work: There is no previously published work on provably secure zk-rollup solutions. The Hydra Head paper [IHT-1.1] studies scalability through state-channels.

References: [IHT-1.1] Hydra: Fast Isomorphic State Channels (Chakravarty et al., 2021)

IHT-2: Inter-Head (T1)

Inter-Head extends Hydra's state channel model to support scalable, multi-party layer 2 networks. It enables participants to lock funds on-chain and transact off-chain with minimal on-chain footprint. This allows for efficient, high-volume interactions, from simple payment channels to complex, isomorphic multi-party channels. Inter-Head aims to create secure, composable layer 2 networks that support diverse decentralized applications while maintaining rigorous cryptographic assurances.

Research goal: The goal is to develop a formal security analysis of Hydra family protocols within the Universal Composability (UC) Framework, providing rigorous security proofs and establishing a foundation for future Hydra-related protocol development.

Applications: A rigorous security analysis of Hydra family protocols and any protocols built upon them. This research thread allows for rigorous security treatment of protocols in the Hydra family as well as protocols that build up on it.

Previous Work: This work builds up on [IHT-2.1] Hydra, [IHT-2.2] Interhead and [IHT-2.3] Canetti's UC framework.

References: [IHT-2.1] Hydra: Fast Isomorphic State Channels (Chakravarty et al., 2021), [IHT-2.2] State Machines across Isomorphic Layer 2 Ledgers (Jourenko et al., 2023), [IHT-2.3] Universally Composable Security: A New Paradigm for Cryptographic Protocols (Canetti et al., 2021)

IHT-3: Optimization tools (T1, T5)

This stream focuses on enhancing the efficiency of Hydra-based Layer 2 networks through optimization tools. It addresses challenges such as fund rebalancing, message routing, and channel synchronization. In multi-party or pairwise channels, imbalances in fund flows can deplete channel capacity, halting transactions even when unused liquidity exists elsewhere. Research will develop mechanisms to mitigate these inefficiencies, ensuring sustained throughput and better resource allocation. By optimizing channel operations, this work supports Hydra's scalability goals while improving network responsiveness, reliability, and the overall user experience in high-demand scenarios.

Research goal: The goal is to develop companion protocols for the Hydra Suite through a three-phase research approach: (1) survey existing literature to identify gaps and compare current tools used in non-Hydra layer 2 protocols with the needs of Hydra; (2) assess compatibility between identified protocols and Hydra's architecture; and (3) design and define new tools to fill those gaps and extend Hydra's functionality.

Applications: The immediate application of this research thread is to develop a set of companion protocols for the Hydra suite of protocols.

Previous Work: Two potentially outdated surveys, [IHT-3.1] and [IHT-3.2], can serve as starting points for the initial review of Layer 2 tool protocols.

References: [IHT-3.1] SoK: A Taxonomy for Layer-2 Scalability Related Protocols for Cryptocurrencies (Jourenko et al., 2019), [IHT-3.2] SoK: Layer-Two Blockchain Protocols" (Gudgeon et al., 2019)

IHT-4: Auditing tools (T1, T10, T11)

Layer 2 protocols like Hydra improve scalability by enabling off-chain transactions, only settling on layer 1 when necessary. While efficient, this privacy can hinder transparency and accountability and thus adoption by institutional players. This stream introduces an optional audit mode for Hydra, allowing accredited auditors controlled and limited insights into the transaction history or predicates about it., thereby balancing privacy with auditability—ensuring that off-chain activity isn't entirely opaque while maintaining user confidentiality. This supports compliance, trust, and regulatory alignment without compromising the scalability benefits of layer 2 solutions.

Research goal: This research has three goals: (i) to implement a practical and easily deployable audit feature for the existing Hydra Head protocol, (ii) to explore from first principles the optimal balance between accountability and privacy in layer 2 solutions, (iii) to design a generalized auditable state-channel protocol that meets these requirements and can be applied beyond the Cardano ecosystem.

Applications: Isomorphic layer 2 execution environments that settle on the Cardano mainchain, enabling regulated institutions to prove policy compliance and pass audits while preserving user privacy to the greatest extent possible.

Previous Work / References: Our ongoing work represents the first effort to introduce auditability to Layer 2 systems. While various auditing approaches have been proposed for transaction-based and account-based blockchains—including in the context of CBDCs—none are directly applicable to the unique characteristics and challenges of layer 2 protocols.

(vii) Interchains

A blockchain ecosystem gains in functionality when it is capable of interoperating with other systems, including other blockchain ecosystems, legacy systems, and the physical world.

Nevertheless, the integration of this functionality has been fraught with problems and attacks, as exemplified by attacks against blockchain bridges in the last few years. This highlights the importance of evidence based engineering and the minimization of the trust assumptions needed for interoperability.

The Cardano ecosystem could benefit from several research directions in the context of interoperability.

IC-1: State proofs and blockchain bridges (T5)

A bridge enables the transfer of assets, tokens, and other information from one blockchain/ledger to another. Ideally the bridge transfers sufficient information about the full ledger state (e.g., in a committed form), so that arbitrary queries about it can be done from another ledger. Two types of commonly considered bridges are trustless bridges, placing no (or very minimal) trust assumptions on the parties

involved, and committee-based bridges, which, for example, could assume honest parties operating the bridge hold the majority of the stake. Due to several high-profile attacks on committee-based bridges, our emphasis will be on trustless bridges. We will however consider the relative benefits of committee-based bridges, as well as bridges that utilize Trusted Execution Environments (TEEs).

Research goal: This proposal focuses on three core research goals related to blockchain bridges; (i) It aims to formally analyze their security, functionality, and construction using standalone (game-based) and composable (UC) frameworks, with a particular focus on the requirements of the Cardano–Midnight bridge. (ii) It will develop efficient zero-knowledge tooling to support state transition proofs and consensus certificates, with significant emphasis on optimizing the underlying arithmetized circuits. (iii) The project will explore the use of Trusted Execution Environments (TEEs) to simplify and accelerate the development of trustless bridge infrastructure.

Applications: Applications that are connected to the Cardano ecosystem. There are wider relations with the Hydra Tail, Minatour, Mithril, and partnerchains.

Previous Work: Relevant works include those on Proof-of-stake Sidechains [IC-1.2], Mithril [IC-1.4], and Cross-chain Communication [IC-1.3]. A further relevant paper is zkBridges [IC-1.1]—Bridges have close relations with the Hydra Tail, Minatour, Mithril, and sidechains projects.

References: [IC-1.1] zkBridge: Trustless Cross-chain Bridges Made Practical (Xie et al., 2022), [IC-1.2] Proof-of-Stake Sidechains (Gaži et al., 2019) [IC-1.3] SoK: Communication Across Distributed Ledgers (Kiayias et al., 2023) [IC-1.4] Mithril: Stake-based Threshold Multisignatures (Kiayias et al., 2024)

IC-2: Privacy preserving and cross-chain DApps and oracles (T3, T9)

The aim is to develop a cryptographic DApp support toolset that includes privacy-preserving data processing for Cardano Smart Contracts and the external oracle secure integration. Smart contracts can be used to orchestrate numerous types of protocols [5]. Blockchain aided orchestration via smart contracts can leverage multi-party computation to create novel decentralized applications, including sophisticated Privacy Enhancing Technology aided Decentralized Finance (DeFI) applications. Furthermore, external oracles can influence smart contract execution with real world data, thus they can also be leveraged in such a framework to feed the integrated system with private information.

Research goal: The primary goal is to develop a framework for efficient and privacy-preserving execution of Cardano smart contracts, enabling the orchestration of decentralized applications that integrate external oracle data on top of the Cardano blockchain.

Applications: The immediate application of this research is to implement a layer that enables the secure deployment of decentralized applications—potentially leveraging privacy-preserving smart contracts—on top of the consensus layer, while integrating trusted information from external sources.

Previous Work: While there are many examples of orchestrating MPC protocols on top of blockchains, the novelty of this research lies in its potential to leverage recent advancements in Cardano's layer 2 protocols—such as [IC-2.1] and [IC-2.2] —to improve efficiency. By utilizing the flexibility and agility of layer 2, the proposed protocol can achieve more scalable and responsive execution.

References: [IC-2.1] State Machines across Isomorphic Layer 2 Ledgers (Jourenko and Larangeira, 2023), [IC-2.2] Hydra: Fast Isomorphic State Channels (Chakravarty et al., 2021), [IC-3.3] The Extended UTXO Model (Chakravarty et al., 2020)

IC-3: Light client infrastructure (T6, T7)

The Cardano ecosystem lacks a foundational approach to light client functionality, including state proofs critical for applications like trustless zk-bridges. Secure, incentivized light clients—essential in protocols like IBC—remain an open challenge, as seen in ongoing discussions around Mithril. This stream aims to develop a future-proof light client infrastructure that addresses asymmetric data retention, device limitations (bandwidth and processing), and end-to-end latency requirements, all supported by robust incentive mechanisms.

Research goal: This research aims to explore the secure, decentralized design of light clients—clients that, ideally, provide similar security guarantees to full nodes without relying heavily on third-party services. Given bandwidth and storage limitations, some trade-offs are inevitable, and this work will evaluate various approaches to balance security, decentralization, and practical constraints.

Beyond core light client design, the research also examines the broader future of client infrastructure in blockchain applications. As ledger state and chain history grow, not all nodes will be able to support even basic wallet functionality. This raises key questions about secure and fair query mechanisms for accessing blockchain data, including how such services can be compensated within a game-theoretic framework.

Additionally, for light clients to remain competitive—especially when interacting with smart contracts—they must meet latency expectations. Thus, this thread will also investigate efficient notification systems that alert light clients to relevant on-chain events without requiring constant processing of the full blockchain.

Applications: Applications within Cardano will be a novel light client with minimal trust assumptions (compared to third-party solutions) that, at the same time, still support smart contracts and DApp development.

Previous Work: Research on light clients remains limited, with relevant papers listed in the references section (as of November 2024). Notably, there is a significant gap in the literature addressing light clients that must re-establish ledger state after prolonged offline periods.

References: [IC-3.1] SoK: Blockchain Light Clients, [IC-3.2] SNACKs: Leveraging Proofs of Sequential Work for Blockchain Light Clients, [IC-3.3] Aurora-Trinity: A Super-Light Client for Distributed Ledger Networks Extending the Ethereum Trinity Client, [IC-3.4] Accountable Light Client Systems for PoS Blockchains, [IC-3.5] ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution, [IC-3.6] A Tendermint Light Client, [IC-3.7] Proofs of Proof-of-Stake with Sublinear Complexity, [IC-3.8] Generic Superlight Client for Permissionless Blockchains, [IC-3.9] Security Properties of Light Clients on the Ethereum Blockchain

IC-4.1 DApp Tokenomics (T3, T5)

Launching a new application, system or partnerchain often involves a critical initial phase that determines the project's success or failure. This study will explore fundamental principles of tokenomics as they apply to the launch of new decentralized applications. Here, ""decentralized application"" refers to a scenario where an existing ""mainchain"" supports the new decentralized application, system or partnerchain during its initial launch phase.

Research goal: The research aims to identify key parameters in different launch designs for a DApp, system of partnerchain that influences its success. These parameters include: (i) partial utilization of mainchain resources, (ii) coexistence of mainchain and partnerchain tokens, (iii) trade-offs between initial investment by the designer and other factors, and (iv) mutual benefits for both parties.

Applications: Provide tools to design an optimal launching phase for a DApp, system or partnerchain, as well as to decide the conditions under which the launching phase terminates and the new entity can operate fully autonomously in economics terms (typically, it can resist external shocks like more mature applications or systems, and its overall economy justifies interoperability with other applictaions or systems, e.g., bridges and decentralized exchanges).

Previous Work: Existing tokenomics models (see below) suffer from two major limitations: (i) they focus only on long-term analysis, while here we need to consider a finite horizon initial launching phase, and (ii) they usually assume users whose individual impact on the economics of the system is negligible. This assumption becomes unrealistic when dealing with new DApps or systems whose economic “weight” can potentially influence the one of the mainchain. Finally, the nature of the questions here has some similarities with the “initial public offer” literature).

References: [IC-4.1] Would Friedman Burn your Tokens? (Kiayias et al., 2024), [IC-4.2] Blockchain Platform Design under Market Frictions (Häfner, 2023), [IC-4.3] Tokenomics: Dynamic Adoption and Valuation (Cong et al., 2021), [IC-4.4] The Value of Decentralization Using the Blockchain (Reuter, 2022). [IC-4.5] Single-token vs Two-token Blockchain Tokenomics (Kiayias et al., 2024)

- **Initial public offerings:** [IC-4.6] Informational asymmetries, financial structure, and financial intermediation (Leland & Pyle, 1977), [IC-4.7] English auctions with resale: An experimental study (Georganas, 2011).

IC-4.2: Consensus Innovation (T6, T7)

This stream explores the next generation of blockchain consensus protocols for Cardano, building on advances from both cryptography and distributed systems. It examines and extends two main paradigms: Nakamoto-style consensus, which relies on probabilistic chain extension, and BFT-style consensus, adapted from classical fault-tolerant systems like PBFT. The research will refine existing models and investigate novel paradigms to improve scalability, security, and decentralization. This includes rethinking and reducing the synchronous assumptions in Ouroboros as well as porting the DAG-based protocols to the blockchain setting with dynamic availability of participants.

Research goal: The goal of this research is to develop novel technology that will ultimately be integrated into a PartnerChains product, with research efforts supporting the design and development of key artifacts—such as formal specifications. At its core, this research focuses on advancing blockchain consensus mechanisms, particularly exploring new proof-of-stake models that offer greater resilience or efficiency compared to existing protocols.

Applications: Within Cardano, this research will support all projects requiring input on consensus layer design, with a particular focus on PartnerChains.

Previous Work: A rich body of literature has developed to optimize BFT-style consensus algorithms, such as HotStuff, Jolteon, Simplex. A very recent and new type of algorithm are the so-called DAG-based consensus algorithms including Bullshark [IC-4.2.2], Narwhal&Tusk [IC-4.2.4], or Shoal [IC-4.2.5]. All these algorithms are presented in semi-synchronous or even asynchronous networks, but with a static validator set.

References: [IC-4.2.1] IOG Innovation workstream, [IC-4.2.2] Bullshark: DAG BFT Protocols Made Practical (Spiegelman at al., 2023), [IC-4.2.3] Bullshark: The Partially Synchronous Version (Spiegelman at al., 2023) [IC-4.2.4] Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus (Danezis et al., 2021), [IC-4.2.5] Shoal: Improving DAG-BFT Latency And Robustness (Spiegelman at al., 2023)

(viii) Core Zero-Knowledge Capabilities

Standardizing a common technical core for all zero-knowledge instances in the Cardano ecosystem, including light-client infrastructure, state proofs, blockchain bridges, proofs of useful work, and also Hydra Tail is an important research direction in its own right.

First, a critical aspect is to ensure its updateability and sustainability. The design of zero-knowledge protocols is a very active field of current development and thus, no matter the protocol that is implemented at any given time, it is inevitable that, for the foreseeable future, one would have to transition to newer protocols that would stem from upcoming research developments.

For this reason, it is important to ensure that the zero-knowledge tooling is “pluggable” and easily updatable so that the Cardano ecosystem can keep up with the most recent developments in ZK systems and do so in a safe fashion.

ZK-1: Core Zero-knowledge capabilities (T1, T6, T8)

Standardizing a common technical core for all zero-knowledge instances in the Cardano ecosystem, including light-client infrastructure, state proofs, blockchain bridges, and also Hydra Tail is an important research direction. Due to internal and external interest in ZK and succinct argument technology, it is important that Cardano specific ZK capabilities are built by strengthening the ties of the Cardano community with the broader ZK engineering and research community. As ZK is a new, highly specialized, and quickly evolving domain, the boundaries between engineering and research are fluid. One means of solidifying engineering practices is active engagement in standardization efforts, for instance of the Halo2 proving system, which can be seen as an evolution and generalization of Plonk.

Research goal: Ensuring the long-term sustainability and upgradability of Cardano's cryptographic algorithms is essential, especially as zero-knowledge (ZK) protocols continue to evolve rapidly. To remain current and secure, Cardano's ZK tooling must be modular and easily updateable, enabling seamless integration of future advancements.

Another key goal is expanding ZK capabilities within Plutus smart contracts—initially for specific use cases like state proofs, and eventually for arbitrary contract logic. Integrating ZK proofs into Plutus would significantly enhance smart contract functionality. A major future milestone is enabling proofs of arbitrarily long computations through recursive proofs and folding schemes, allowing efficient and verifiable computation on-chain.

Applications: ZK technology enables succinct on-chain proofs of off-chain computation, supporting not just privacy but also scalability and trust across domains like gaming, data provenance, governance, and financial services—making it essential for seamless blockchain integration.

Previous Work / References: The BTL ZK Lab has conducted research on the simulation-extractability of leading SNARK proof systems such as Plonk and Marlin, as well as on inclusive accountability mechanisms and formal security models for anonymous credentials that leverage general-purpose zero-knowledge proofs.

(ix) The Post-Quantum Landscape

Recent advancements in quantum computing technology suggest that any system that aspires to long-term sustainability must withstand anticipated attacks that leverage quantum technology.

While protecting the ecosystem from quantum threats to security is the major motivation of these activities, quantum technology may also provide important new techniques to improve the security and performance of blockchain infrastructure.

Below we outline these two broad research directions in the context of Cardano.

PQL-1: Post-quantum readiness (T6)

Current security analyses of Cardano protocols and their underlying cryptographic primitives largely assume classical attackers. However, ongoing global efforts to build scalable quantum computers pose a significant threat to many standard cryptographic schemes (e.g., RSA, DSA, Schnorr), which will be broken once such machines are realized. To future-proof Cardano, it is essential to design, evaluate, and integrate cryptographic tools that provide rigorous post-quantum security.

This effort consists of two core threads. The first focuses on designing and integrating post-quantum cryptographic primitives. While some components, like signatures and hash functions, already have well-studied quantum-secure alternatives, others—such as Verifiable Random Functions (VRFs) and threshold signatures—require new research to balance security, efficiency, and deployability.

The second thread addresses the security of higher-level protocols, such as Ouroboros, under quantum adversaries. This is particularly complex when critical components—like nonce generation in Ouroboros

Praos—depend on lower-level cryptographic assumptions. Addressing this challenge requires the development of new analytic tools and a protocol-specific analysis of Cardano's architecture.

Key performance indicators include the computational and parameter overhead introduced by post-quantum primitives relative to their classical counterparts, and the adjustments needed in protocol parameters to maintain security in a post-quantum setting.

Research goal: The advent of scalable quantum computers will undermine many foundational elements of today's public-key infrastructure. While hash-based signatures—already used in Cardano—offer post-quantum security, there is currently no unified approach for developing quantum-resistant alternatives to all cryptographic tools. Promising methods based on lattices or error-correcting codes can support a range of primitives but often face significant efficiency trade-offs.

This research stream focuses on building a comprehensive post-quantum cryptographic toolkit for Cardano, starting with the consensus layer. While some components, like hash-based signatures, already consider quantum threats, others—such as Verifiable Random Functions (VRFs)—remain poorly understood and require foundational research. Additionally, aspects like randomness generation via hashing (e.g., nonce generation) must be re-evaluated under quantum threat models.

Beyond consensus, the stream may also address broader cryptographic needs in Cardano, including threshold signatures and zero-knowledge proofs, with the aim of ensuring long-term security and efficiency across the system—even under quantum adversaries.

Applications: Cardano and ecosystem

Previous work / References: The cryptographic community has developed a robust set of hash-based signature schemes with strong post-quantum security guarantees, and significant progress has been made in improving their efficiency—some of which are already deployed in Ouroboros. However, post-quantum secure Verifiable Random Functions (VRFs), another core component of the protocol, remain less well understood. Current solutions lack an effective balance between flexibility and efficiency, and most security analyses are based on classical adversaries using assumptions believed to hold in a post-quantum world. Additionally, when it comes to analyzing the security of the full protocol—particularly nonce generation—existing methodologies offer only limited insights, leaving important questions unresolved.

PQL-2: Post-quantum enhancements (T6)

While quantum computing poses serious risks to classical cryptography, it also offers new opportunities to enhance security and performance. Recent work on *one-shot signatures* [1] illustrates this potential, showing how the no-cloning theorem, combined with cryptographic techniques, can enable keys that are usable for a single signature and then self-destruct—providing strong guarantees against misuse.

These signatures can be transmitted and verified using classical means, requiring only local quantum computation without the need for quantum communication or persistent quantum memory. This makes them practical for short-term use and potentially valuable for blockchain applications, particularly in strengthening proof-of-stake security and improving performance in critical operations.

Key performance indicators (KPIs) for this stream include the computational complexity of the required quantum operations and the feasibility and cost of producing quantum devices capable of supporting such primitives. Additionally, advancements in quantum key distribution (QKD)—likely to become practical before full-scale quantum computing—may provide new tools for secure, high-value key management within the Cardano ecosystem.

Research goal: This research stream will initially focus on evaluating the feasibility and efficiency of one-shot signatures, while also exploring other quantum information and computation techniques that could offer high value to the Cardano ecosystem. A key challenge will be balancing potential benefits with the expected timeline for the availability of necessary quantum hardware. Given that the practicality of one-shot signatures depends heavily on the computational complexity of the quantum signing process, reducing this complexity will be a central priority.

Applications: One-shot signatures could deliver forward-secure digital signatures for the Ouroboros protocol, enhancing protection against long-range attacks without relying on external key erasure mechanisms. Their deployment would significantly strengthen consensus layer security. Additionally, quantum key distribution may offer new, more secure methods for managing and distributing high-value cryptographic keys.

Previous work / References: Existing work on single-shot signatures establishes theoretical viability, but does not speak to the efficiency of the solution. Existing work on quantum key distribution provides this functionality over small geographic distances, but does not provide sufficient connectivity for large-scale key management.

2.5 Communication

To date, IOR has effectively leveraged IOHK's digital platforms and communication channels to disseminate research, foster collaboration, and engage with a broad range of stakeholders. The IOHK website's Research section offers a clear, accessible overview of IOR's activities and achievements, featuring:

- **About**: Showcasing IO Research's vision, structure, and areas of interest, along with a curated selection of videos highlighting key initiatives.
- **Library**: A searchable and regularly updated repository of over 230 research papers, providing access to groundbreaking studies and findings.
- **Research Topics**: A periodically updated overview of spinouts and research tribes, reflecting the dynamic and evolving focus of the department.

IOR uses IOHK's social media platforms—including X (formerly Twitter), LinkedIn, and Discord—to broaden its reach and amplify its impact. Nine videos featured on the IOHK research page have collectively attracted over 55,000 views on YouTube, and IOR contributed to nine of the 25 IOHK blog posts published in 2024.

These communications highlight researcher insights, protocol developments, and academic partnerships. Additional webinars and events in 2024 included the "11 Blockchain Tenets" X Space and ongoing

participation in high-profile conferences like Rare Evo in Las Vegas and the Cardano Constitutional Convention in Buenos Aires.

Looking ahead to 2025 and beyond, IOR recognises the importance of expanding and deepening its communication strategy. It is collaborating more closely with Intersect to improve engagement with key ecosystem participants, including SPOs, DApp developers, DReps, and Delegates. IOR also aims to enhance the accessibility of its research outputs, including through AI-driven tools, ensuring that its contributions to blockchain innovation are both widely recognised and more seamlessly integrated into the broader Cardano ecosystem.

2.6 Dissemination

The breadth of IOR's contributions is evident in its growing publication record. The Research library now houses over 230 peer-reviewed papers involving more than 150 academics, with around 50 core works underpinning Cardano's five development phases.

In 2024, Research published more than 30 papers, involving over 77 researchers, covering blockchain governance, privacy, cryptographic innovation, and scalability. Our Chief Scientist, Professor Aggelos Kiayias FRSE, a leader in these efforts, received the prestigious BCS Lovelace Medal for his transformative contributions to cybersecurity and cryptography. His work has driven innovations in energy efficiency, interoperability, and privacy, with the Ouroboros consensus protocol—a foundational milestone for proof-of-stake systems—cited over 3,000 times and also adopted by blockchains like Polkadot and Mina.

Research Conferences

IOR is actively involved in the global academic community, showcasing its commitment to advancing blockchain technology through rigorous research and collaboration. Its researchers regularly speak at prestigious international conferences and contribute to the broader discourse on blockchain and decentralized systems. These conferences provide a platform to present the latest research findings for Cardano, engage with other thought leaders and stay at the forefront of technological innovation.

Input Output strategically sponsors a number of these conferences each year, reinforcing its dedication to fostering a vibrant and well-supported academic environment. This enhances the visibility and positioning of both Cardano and Input Output within the research community and also acts as a talent magnet to help cultivate the next generation of blockchain researchers. This involvement ensures that IOR continues to set the standard for excellence in the field, driving forward the development of Cardano and the broader blockchain ecosystem via conferences including those outlined below.

Cryptography

- **ASIACRYPT**: A major international conference organized by the International Association for Cryptologic Research (IACR), dedicated to the field of cryptology and information security, featuring the latest research in cryptographic algorithms and protocols.

- **EUROCRYPT: O**ne of the premier annual conferences organized by the International Association for Cryptologic Research (IACR), focusing on cryptographic research and its applications, featuring the latest advances in cryptography from around the world.

- **CRYPTO:** A flagship conference of the International Association for Cryptologic Research (IACR), focusing on the latest advancements in cryptography, including cryptographic theory, techniques, and applications.

- **Financial Cryptography and Data Security (FC):** An interdisciplinary conference that explores the intersection of cryptography, data security, and financial systems, addressing critical topics such as blockchain technology, digital currencies, and privacy.

Security

- **Computer and Communications Security (CCS):** A leading conference organized by ACM / SIGSAC (Association for Computing Machinery / Special Interest Group on Symbolic & Algebraic Manipulation) that focuses on all aspects of computer and communications security, featuring cutting-edge research in cybersecurity.

- **IEEE Security and Privacy "Oakland":** An influential annual event that focuses on the latest advancements in security, privacy, and cryptography. Renowned for its rigorous review process, Oakland is considered one of the top venues for presenting cutting-edge research in cybersecurity and privacy.

- **USENIX Security Symposium:** A premier annual conference focused on the latest research in computer security and privacy, including network security, applied cryptography, web security, malware, and privacy-enhancing technologies.

- **Network and Distributed System Security Symposium (NDSS)**: An annual conference focused on the latest research in network and distributed system security, featuring peer-reviewed papers, keynotes, and workshops that address contemporary security challenges and innovations in areas such as cryptography, privacy, and secure protocols.

Programming Languages

- **Formal Methods in Blockchain (FMBC)**: A specialized conference dedicated to the application of formal methods to blockchain technology, aimed at improving the reliability and security of blockchain systems.

- **Principles of Programming Languages (POPL):** A conference that focuses on fundamental principles and innovations in programming languages, including their design, implementation, theory, and applications. It brings together researchers and practitioners from both academia and industry to present cutting-edge work on programming language theory, formal methods, compilers, and related areas.

Game Theory:

- **Symposium on Algorithmic Game Theory (SAGT)**: A conference that focuses on the study of game theory from an algorithmic perspective, exploring the computational aspects of strategic interaction in economic systems.

- **Workshop on Internet Economics (WINE)**: A leading conference focused on algorithmic game theory and computational economics, bringing together researchers to discuss advances in the economics of the internet.

2.7 Bibliography

In addition to the references cited within individual research streams, the following bibliography includes key academic papers, technical reports, and foundational texts that informed the development of the thematic focus areas for Cardano Vision.

[1] Ryan Amos, Marios Georgiou, Aggelos Kiayias, Mark Zhandry, One-shot signatures and applications to hybrid quantum/classical authentication, STOC 2020

[2] Cardano - Governance https://cardano.org/governance/

[3] Lin William Cong, Ye Li and Neng Wang, Tokenomics: Dynamic Adoption and Valuation, The Review of Financial Studies, Volume 34, Issue 3, March 2021, Pages 1105–1155.

[4] Matthias Fitzi, Xuechao Wang, Sreeram Kannan, Aggelos Kiayias, Nikos Leonardos, Pramod Viswanath, and Gerui Wang, Minotaur: Multi-resource blockchain consensus. ACM CCS, 2022.

[5] Steven Golob, Sikha Pentyala, Rafael Dowsley, Bernardo David, Mario Larangeira, Martine De Cock and Anderson Nascimento, A Decentralized Information Marketplace Preserving Input and Output Privacy, DEC '23.

[6] Samuel Häfner, Blockchain Platform Design under Market Frictions, 2023, Available at SSRN: https://ssrn.com/abstract=3954773

[7] Aggelos Kiayias, and Philip Lazos, SoK: Blockchain Governance, ACM AFT, 2022

[8] Brook Manville and Josiah Ober, In Search of Democracy 4.0: Is Democracy as We Know It Destined to Die?, IEEE Technology and Society Magazine, vol. 38, no. 1, pp. 32-42, March 2019.

[9] Rowan van Pelt, Slinger Jansen, Djuri Baars & Sietse Overbeek, Defining Blockchain Governance: A Framework for Analysis and Comparison, Information Systems Management, 38:1, 21-41, 2021.

[10] Marco Reuter, The Value of Decentralization Using the Blockchain (2022). ZEW - Centre for European Economic Research Discussion Paper No. 22-056, Available at SSRN: https://ssrn.com/abstract=4288348

[11] Bingsheng Zhang, Roman Oliynykov, and Hamed Balogun. A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence, NDSS 2019.

[12] Dimitris Karakostas, Aggelos Kiayias, Christina Ovezik: SoK: A Stratified Approach to Blockchain Decentralization. Financial Cryptography and Data Security 2024.

[13] Michele Ciampi, Aggelos Kiayias, Yu Shen:
Universal Composable Transaction Serialization with Order Fairness. CRYPTO (2) 2024: 147-180

3. Work Program 2025

3.1 Introduction

The 2025 Work Program is organized around nine thematic focus areas, each containing targeted research and innovation workstreams addressing key challenges and opportunities in blockchain. These workstreams are carefully selected to advance groundbreaking technologies and scalable solutions that strengthen Cardano's position as an industry leader. The program supports proactive portfolio management to allocate resources efficiently toward high-impact initiatives, while emphasizing tailored intellectual property (IP) strategies to safeguard and capitalize on innovations.

Each workstream is designed with a clear motivation, outlining the technical challenges to be addressed and the benefits to Cardano. Objectives are well-defined, with expected deliverables such as enhanced protocols, improved interfaces, or new dApp capabilities. Workstreams are scoped to meet essential requirements, including staffing, cost estimates, references, and timelines. This structured approach ensures efficient execution, clear progress tracking, and tangible contributions to Cardano's long-term vision of a secure, scalable blockchain platform.

3.2 Portfolio Approach

Due to the exploratory nature of early-stage research, flexibility is essential. IOR adopts a portfolio-based approach to manage research investments and adjust priorities as needed. This ensures resources are directed to the most promising and strategically aligned workstreams across thematic areas.

The portfolio approach allows for regular assessment of progress, risk, and opportunity, enabling dynamic reallocation of funds where impact is greatest. Projects that show strong potential may be accelerated, while those that no longer align may be scaled back. IOR will communicate significant changes in advance and provide regular progress updates, with formal reviews at mid-year and year-end.

3.3 Fundamental Research Workstreams

IOR proposes 20 research workstreams for 2025, each aligned with Cardano's mission and already demonstrating promising outputs. These workstreams aim to significantly enhance the Cardano platform while addressing broader blockchain challenges. They reflect IOR's commitment to high-impact research that fuels innovation and advances Cardano's strategic goals.

Given the uncertainty inherent in foundational research, workstream priorities will naturally evolve. As new insights emerge, certain streams may rise or fall in relevance. This is expected in rigorous academic processes, where hypotheses are refined and peer-reviewed outputs may undergo multiple revisions before publication in top-tier venues.

This iterative process reinforces the need for a flexible, adaptive research strategy—one that ensures Cardano remains responsive and forward-looking. As these workstreams progress, they will continue to

expand Cardano's research portfolio, providing a rich pipeline of knowledge and innovation to drive the platform's ongoing development.

The World's Operating System

WOS-2: State-machine contract environment

Research Lead: Manuel Chakravarty
Start date: Jan 25
Forecast Duration (months): 24
2025 FTEs: 1.8
Intersect Product Roadmap:: Architectural Excellence

Objectives	1. We propose to realise a prototype EasySM-based programming environment as an embedded language in a sufficiently expressive host language. This could be Agda or Haskell. 2. We propose to define the formal semantics of EasySM in Agda.
Workplan	**Programming environment** T1. How can we embed EasySM in Haskell and/or Agda (Start: M1, Duration: 12 Months) T2. How do we embed the various typing constraints including encoding the underlying DFA (deterministic finite automata) as types (Start: M1, Duration: 12 Months) T3. Define a suitable operational semantics (Start: M1, Duration: 12 Months) T4. Derive a compilation strategy and/or interpreter from the operational semantics (Start: M6, Duration: 18 Months) T5. Implement the interpreter and/or compiler (Start: M6, Duration: 18 Months) **Formal semantics** T6. Define a logical semantics for EasySM in Agda (Start: M6, Duration: 18 Months) T7. Define a suitable operational semantics (Start: M1, Duration: 12 Months) T8. Mechanise the operational semantics in Agda (Start: M6, Duration: 18 Months)
Deliverables	D1. Implementation of the prototype programming environment (for research & expert users, not production) D2. Code generation from EasySM to Plutus code D3. Formal semantics in Agda D4. Programming environment paper D5. Formal semantics in Agda paper
Impact	More convenient smart contract development & engineering for Cardano that facilitates formal reasoning.
Minimal Requirements	The programming framework needs to enable the definition of complex contracts, such as those used in the Hydra project. Moreover, the framework needs to support executing such contracts against a sequence of inputs to generate an execution trace of the contract. On the formal side, the semantics needs to cover all static and dynamic

	aspects of the state-machines defined in the programming environment with transition relations defined in Agda (i.e., we will not model the semantics of the host language).
Team	Research Fellow (Programming Languages), 0.4 FTE (24 Months) Research Fellow (Cryptography), 0.4 FTE (24 Months) Research Engineer, 1.0 FTE (24 Months)

WOS-6: Location-based services and smart contracts

Research Lead: Marc Roeschlin
Start date: Oct 22
Duration (months): 48
2025 FTEs: 1.2
Intersect Product Roadmap: Architectural Excellence, Incoming Liquidity

Objectives	(1) The goal is to develop a location verification primitive and then show its applicability in a blockchain ecosystem. (1+2) The location verification protocol will then facilitate the implementation of geographic diversity and location-based services.
Workplan	T1. Define a location verification primitive (Start: M1, Duration: 18 Months) T2. Analyze protocol charters (Start: M17, Duration: 18 Months) T3. Protocol simulation (Start: M20, Duration: 7 Months) T4. USe case research (Start: M16, Duration 12 Months) T5. (a) Geographic diversity incentivization (b) Framework for smart contract integration (Start: M25: Duration 15 Months) T7. Measurement message reporting (Start: M27, Duration 12 Months) T8. Measurement set VRF (Start: M30, Duration 12 Months) T9. Measurement aggregation & location validation (Start: M32, Duration 12 Months) T10. SPO reward scoring (Start: M36, Duration 8 Months) T11. Protocol location verification (possibly together with Innovations and Engineering) (Start: M40, Duration 8 Months)
Deliverables	D1. Initial paper covering the location verification primitive and protocol (Q4, 24) D2. One or two papers on geographic diversity (2) D3. One or two papers on location-based services (reward sharing and incentivisation) and smart contracts (depending on use cases) (Q4 25). D4. One paper/survey on analyzing geographic diversity of existing blockchains (Q4 26).
Impact	Location information is becoming increasingly important: decentralization, geopolitics, legal, access control, etc. DApps & user growth.

Minimal Requirements	(1) The location verification protocol must implement a functionality that allows the verification of location claims (made on the ledger) up to a predefined geographical accuracy and under adversarial conditions, i.e. tolerating a certain fraction of compromised nodes. (2) A reward sharing scheme that takes location of nodes into consideration and accordingly compensates them, i.e., a node in an underrepresented/remote area should receive higher reward than nodes in an overcrowded area.
Team	Research Fellow (Consensus), 0.4 FTE (48 months) Research Fellow (Distributed systems), 0.4 FTE (48 months) Research Fellow (Protocol design / security), 0.2 FTE (48 months) Research Fellow (Applied cryptography), 0.1 FTE (48 months) Chief Scientist, 0.1 FTE (48 months)

Ouroboros Omega

OO-1V: Peras - Vision

Research Lead: Peter Gaži
Start date: Jan 25
Duration (months): 48
2025 FTEs: 0.9
Intersect Product Roadmap: Scaling the L1 Engine

Objectives	The overarching goal of this line of research is to significantly improve settlement speed of longest-chain protocols in general, without compromising on other appealing security and performance properties these protocols enjoy, including self-healing or being operational under dynamic participation. The research is aimed at producing research papers describing provably secure approaches that balance complexity and efficiency while offering improved settlement times for Ouroboros.
Workplan	D1: Modular improvements of the basic protocol research paper & technical report D2: Integration and synergies with existing technologies research paper & technical report D3: Extensions and generalizations research paper & technical report D4: Understanding tradeoffs and limitations research paper & technical report The above list of research avenues is to be understood as a “menu” from which concrete topics are chosen based on prioritization due to the current product needs and the resource allocation. This will determine the final outcomes and deliverables.
Deliverables	T1: Modular improvements of the basic protocol (Start: M1, Duration 48 months) T2: Integration and synergies with existing technologies. (Start: M1, Duration 48 months) T3: Extensions and generalizations. (Start: M1, Duration 48 months)

	T4: Understanding tradeoffs and limitations. (Start: M1, Duration 48 months)
Impact	The immediate effect would be better user experience for parties transacting on chain. Moreover, such settlement times would also be an enabler for various layer 2 functionalities and for bridging to other blockchains further increasing growth and interoperability.
Minimal Requirements	n/a
Team	Research Fellow (Consensus / Cryptography), 0.2 FTE (48 months) Research Fellow (Consensus / Cryptography), 0.2 FTE (48 months) Research Fellow (Consensus / Cryptography), 0.2 FTE (48 months) Senior Research Fellow (Algorithms), 0.2 FTE (48 months) Chief Scientist, 0.1 FTE (48 months)

OO-2: Leios

Research Lead: Giorgos Panagiotakos
Start date: Jan 22
Duration (months): 42
2025 FTEs: 1.9
Intersect Product Roadmap: Leios

Objectives	(1) Design and analyze an appropriate protocol that allows for scaling throughput (2) To deal with any concurrency issues arising in such a high rate setting (3) Consider compatibility with Ouroboros Peras (4) To allow for optimistic fast transaction settlement, as well as how to deal with congestion control in a highly concurrent system
Workplan	T1. Describe a blockchain protocol whose throughput scales vertically. (Start: M1, Duration: 30 months – Completed, paper [4] under submission). T2. How does the protocol deal with concurrently produced blocks containing conflicting transactions? How can we prevent or minimize the inclusion of conflicting transactions? (Start: M36, Duration: 12 months) T3. (a) Is the current transaction diffusion layer suitable for highly concurrent block production? If not, design a new transaction diffusion layer. (Start: M36, Duration: 12 months) T3. (b) How can we merge Ouroboros Leios with Ouroboros Peras and retain the guarantees provided by both protocols? (Start: M36, Duration: 6 months) T4. Design suitable congestion control mechanisms for a concurrent setting. How can we adapt EIP-1559 to work in this case? Is Tiered Pricing a suitable choice? (Start: M36, Duration: 6 months)

Deliverables	At least three research papers (targeting top-tier conferences): D1. How to scale data throughput D2. Concurrency issues such as minimizing the inclusion of conflicting transactions in concurrently produced blocks D3. The design of the network layer of high throughput protocols
Impact	Increase throughput in order to develop the ecosystem (partnerchains, etc)
Minimal Requirements	The throughput of Leios should be proportional to the resources SPOs are required to have. E.g., currently SPOs are assumed to have "..1 GB of bandwidth per hour..", see https://developers.cardano.org/docs/operate-a-stake-pool/hardware-requirements/
Team	Research Fellow (Networking), 0.4 FTE (42 months) Research Fellow (Consensus), 0.6 FTE (42 months) Senior Research Fellow (Consensus), 0.4 FTE (42 months) Research Fellow (Consensus), 0.4 FTE (42 months) Chief Scientist, 0.1 FTE (42 months)

OO-3: Fair transaction processing

Research Lead: Aggelos Kiayias
Start date: July 24
Duration (months): 42
2025 FTEs: 1.6
Intersect Product Roadmap: Scaling the L1 Engine, Incoming Liquidity

Objectives	(1) Design and analyze the suitable extension / overlay of Ouroboros for fair transaction processing. (2) Ensure compatibility with Peras and Leios
Workplan	T1. Develop the appropriate definitions for fair transaction processing (Start M1: Duration 12 months. task complete see reference [13]). T2. Protocol design space exploration. Develop different protocols and compare and contrast performance and effectiveness. (Start M1, Duration 36 months, task underway). T3. Investigate and adapt networking layer and mechanism design elements to ensure the designs are incentive compatible (Start M12, Duration 36 months). T4. How can we merge the resulting protocols with other parallel threads to layer 1 and layer 2 including Ouroboros Leios and Ouroboros Peras? (Start: M24, Duration: 24 months)

Deliverables	Three research papers targeting top tier conferences on: D1. Protocol Design for fair transaction processing. D2. Networking design for Fair transaction processing. D3. Mechanism design for fair transaction processing.
Impact	If successful, this research could become a unique selling point for Cardano, as no public blockchain currently offers fair transaction processing.
Minimal Requirements	n/a
Team	Research Fellow (Consensus), 1 FTE (42 months) Research Fellow (Networking), 0.5 FTE (42 months) Chief Scientist, 0.1 FTE (42 months)

OO-5: Multi-resource consensus - Minotaur

Research Lead: Matthias Fitzi
Start date: Jan 25
Duration (months): 24
2025 FTEs: 1.3
Intersect Product Roadmap: Architectural Excellence, Incoming Liquidity

Objectives	The goal is to construct a provably secure multi-resource consensus protocol for sidechains including respective components for reliable communication of mainchain state information to the sidechain.
Workplan	T1. A stake-delegation mechanism for Cardano to allow for sidechain restaking (Start: M1, Duration 24 months) T2. A staking bridge for each external staking source to reliably inform the sidechain about the amount and distribution of dedicated stake (Start: M1, Duration 24 months) T3. A dynamic mechanism to balance the power of each stake source, i.e., how much control is assigned to the stakers from each source (over time) (Start: M1, Duration 24 months) T4. A mechanism for reward distribution to the restaking entities (Start: M1, Duration 24 months)
Deliverables	D1. A research paper describing a provably secure implementation of multi-resource BFT consensus or components thereof—to be published at a renowned security or cryptography conference if publishable—otherwise a technical report or eprint paper.
Impact	Multi-resource sidechains consensus will make it easy to bootstrap new Cardano sidechains, helping to attract them to the Cardano ecosystem.

Minimal Requirements	A sidechain protocol is to be devised where block-production rights are controlled via the staking from two (or more) different stake sources—implying the restaking of those controlling assets that are non-native to the sidechain..
Team	Senior Research Fellow (Consensus), 0.5 FTE (24 months) Research Fellow (Layer 2), 0.4 FTE (24 months) Research fellow (Consensus / Cryptography), 0.4 FTE (24 months)

OO-6: Proofs of useful work

Research Lead: Giorgos Panagiotakos
Start date: Jan 25
Duration (months): 24
2025 FTEs: 0.8
Intersect Product Roadmap: Architectural Excellence

Objectives	1. Address remaining challenges in optimization-based Proofs of Useful Work (PoUWs), such as those in [1]. 2. Explore the applicability of PoUWs to other domains, including SNARKs and machine learning. 3. Investigate economic models and incentive structures for PoUW-based blockchains. 4. Examine how privacy features can be integrated into PoUW blockchain designs.
Deliverables	T1. Provide a PoUW for optimization that has state-of-the-art performance in terms of the optimization algorithm implemented. (Start: M9, Duration: 15 months, Completed. Paper under submission, not yet public.) T2. How to argue about the moderate hardness of (somewhat randomized) local search computations? (Start: M48, Duration: 9 months) T3. How to deal with malicious optimization problem injection attacks, where the attacker plants a trapdoor in the problem in order to be able to cheaply perform local search computations? (Start: M48, Duration: 9 months) T4. How general can the statements encoded in PoUW-SNARKs be? (Start: M48, Duration: 12 months) T5. Can we distribute the production of PoUW-SNARKs into smaller work chunks while maintaining security? (Start: M48, Duration: 12 months) T6. Are secure PoUWs for machine learning at all feasible? How can we deal with large datasets (and their availability) that cannot be replicated across the network? (Start: M48, Duration: 12 months) T7. How to argue about the moderate hardness of (somewhat randomized) ML computations? (Start: M48, Duration: 9 months) T8. Design an appropriate incentives framework for PoUW blockchains. (Start: M48, Duration: 12 months) T9. How should a marketplace for PoUW problems be set up? How to incentivize

	miners to solve problems from the marketplace? How to incentivize miners to publish their solution on the blockchain instead of doing off-chain deals with the problem setter? (Start: M48, Duration: 12 months) T10. Provide a mechanism for the problem setter to hide/obfuscate the details of the problem he wants to solve (Start: M48, Duration: 12 months). T11. Can the PoUW solutions provided by miners be only known to the problem setter? (Start: M48, Duration: 12 months)
Workplan	D1. Ofelimos: Combinatorial Optimization via Proof-of-Useful-Work (Crypto 2022) D2. Proof-of-Useful Work is Practical: Consensus via a Competitive Optimization Engine (under review) D3. Paper on why the local search computations employed by the previous papers produced (or some variant of them) are moderately hard. D4-D5. Depending on the interest in PoUWs for SNARKs or ML additional papers may be produced outlining suitable protocols to use in these two cases.
Impact	A PoUW protocol for optimization problems that is both performant, in terms of the optimization part, and secure, in terms of the blockchain/PoUW part.
Minimal Requirements	In terms of impact, we expect PoUW-based blockchain to attract high-value industrial businesses into our ecosystem, as they are in need of regularly solving optimization problems cheaply, e.g., transportation companies.
Team	Research Fellow (Networking), 0.2 FTE (60 months) Research Fellow (Consensus), 0.1 FTE (60 months) Senior Research Fellow (Consensus), 0.1 FTE (60 months) Senior Research Fellow (Optimisation/Local Search), 0.2 FTE (60 months) Research Fellow (Consensus), 0.1 FTE (60 months) Chief Scientist, 0.1 FTE (60 months)

OO-7: Congestion control

Research Lead: Giorgos Panagiotakos
Start date: Jan 22
Duration (months): 60
2025 FTEs: 1.7
Intersect Product Roadmap: Scaling the L1 Engine, Incoming Liquidity

Objectives	Expand our understanding of congestion control mechanisms that consider user urgency and application diversity (O1), predictability (O2), and resource heterogeneity (O3). Tiered pricing as well as resource heterogeneity lead to designs with a large number of parameters that need to be tuned to current demand. We may additionally research how the parameter update process should work in order to guarantee fast convergence. (O4)

Workplan	T1. Design a congestion control mechanism that takes in account user urgency and ensures the blockchain serves a diverse set of applications, i.e., from low (e.g., payment channel maintenance) to high (e.g., DeFi) urgency ones. (Start: M1, Duration: 24 months – Completed. [1]) T2. (a) Design a predictable service mechanism based on (i) tokenizing the available throughput, (ii) distributing it to interested parties through an auction, and (iii) ensuring predictable delays based on the obtained tokens. (Start: M1, Duration: 24 months – Completed. [3]) T2. (b) Design a predictable service mechanism based on a blockchain space futures mechanism. (Start:M30, Duration: 6 months) T3. (a) How to handle multi-resource congestion? (Start:M30, Duration: 12 months) T3. (b) How to handle semi-permanent resources such as file storage. (Start:M36, Duration 12 months) T4. How should the parameter update process work in order to ensure rapid convergence? (Start: M36, Duration 6 months)
Deliverables	D1. Tiered Mechanisms for Blockchain Transaction Fees (Kiayias, Koutsoupias, Lazos, Panagiotakos) MARBLE 24 D2. (a) Blockchain Space Tokenization, AFT 24 D2. (b) A paper on auctions and predictable delays (in progress) D3. (a) A paper on multi-resource congestion D3. (b) A paper on semi-permanent resources D4. (a) A paper on parameter updates This research stream is expected to produce 2-4 research papers presented at well-established economics, security or blockchain venues exploring the tasks outlined in the previous section. 2 papers have already been published ([1],[3]) exploring Objectives 1 and 2. An additional paper is expected for task 3 and at least one more paper is expected for Objective 3.
Impact	A successful design would enable increased ecosystem growth due to the ease of participation for a variety of applications, e.g., low urgency, business, DeFI.
Minimal Requirements	We aim to present a modular congestion control architecture that can deal with application diversity, service predictability, and resource heterogeneity, in addition to publishing research about the provided properties and guarantees.
Team (Staffing)	Research Fellow (Consensus), 0.4 FTE (60 months) Senior Research Fellow (Consensus), 0.1 FTE (60 months) Research Fellow (Consensus), 0.1 FTE (60 months) Research Associate, 0.5 FTE (12 months) Research Associate, 0.5 FTE (12 months) Chief Scientist, 0.1 FTE (60 months)

Tokenomicon

TO-1: Tokenomics design

Research Lead: Paolo Penna
Start date: Jan 25
Duration (months): 48
2025 FTEs: 1.4
Intersect Product Roadmap: Architectural Excellence, SPO Incentive Improvements

Objectives	Investigate and compare a number of practical solutions currently implemented by Cardano and other systems, and their main differences, advantageous, and potential weaknesses.
Workplan	T1. Provide a mathematical model for tokenomics design which incorporates Cardano's design features (Start: M1, Duration: 6 Months): reserve monetary policy, treasury, transaction fee mechanisms, reward sharing schemes. T2. Establish trade-offs between different parameter combinations and system goals (Start: M7, Duration: 18 Months): security of PoS, token inflation, token price evolution over time. T3. Include Cardano ecosystem in the tokenomics model, e.g., (i) sidechains and their impact on the main chain economics and PoS security,(ii) multi-token systems, their advantages, and optimal designs (Start: M25, Duration: 18 Months). T4. Dynamic models that capture (i) dynamic adoption, (ii) external shocks and (iii) the ability of the system to react / reist to such external factors / changes (Start: M25, Duration: 18 Months).
Deliverables	Four research papers targeting top-tier conferences: D1. Cardano's key parameters D2. The ecosystem as a whole, including side-chains and multi-token platforms. Following the achieved results, we shall research and develop new tokenomics designs incorporating: D3. Dynamics aspects mentioned above D4. Further economics security features that can cope with highly sophisticated algorithms and investment strategies, e.g., so-called (post) modern portfolio theory, and restaking opportunities.
Impact	Economic, adoption and ecosystem growth, more diverse and broader tokenomics capabilities, improved governance.
Minimal Requirements	The new mathematical models developed with this research shall consider the heterogeneous and decentralized nature of Cardano and its ecosystem. These models will inform about the ability of the system to reach and maintain a desired long-term equilibrium and thus to perform as intended.

Team (Staffing)	Research Fellow (Game Theorist), 0.3 FTE (48 Months) Research Fellow (Tokenomics), 0.4 FTE (48 Months) Research Fellow (Economist), 0.4 FTE (48 Months) Chief Scientist, 0.1 FTE (48 Months)

TO-2 Rewards sharing and transaction fees

Research Lead: Evangelos Markakis
Start date: Jun 23
Duration (months): 48
2025 FTEs: 0.4
Intersect Product Roadmap: Architectural Excellence, SPO Incentive Improvements

Objectives	The goal is to obtain a deeper understanding on the intricacies and game-theoretic aspects regarding the design of reward mechanisms. We expect this effort will eventually lead to proposing solutions that would enhance the currently deployed reward sharing scheme of Cardano.
Workplan	T1. Study of alternative reward schemes in on-chain pooling (Start: M1, Duration: 30 Months) T2. Comparisons between on-chain and offchain pooling (Start: M12, Duration: 18 Months) T3. Study of variance in reward schemes (Start: M18, Duration: 18 Months) T4. Applications to other reward mechanisms within Cardano (Start: M30, Duration: 12 Months) T5. Development of a user tool (Start: M30, Duration: 18 Months)
Deliverables	Technical reports or research papers submitted for publication to relevant conferences, either on blockchain technology aspects or specialized towards algorithmic game theory and incentives. D1. Paper on the study of alternative reward schemes D2. Paper on on-chain vs offchain pooling D3. Paper on the study of variance in reward schemes D4. User tool
Impact	The outcome of this research is aimed at improving in the long term the current reward sharing scheme of Cardano, which is an important component of the entire protocol. This in turn can affect user experience and satisfaction. Furthermore, this research has the potential to create impact for other types of payment schemes that are used within Cardano, such as the Voltaire dRep rewards or the rewards issued for reviewers and delegates under project Catalyst.
Minimal Requirements	We aim to propose alternative reward mechanisms and provide comparisons (either via mathematical analysis or via simulations or both) against each other and against the existing scheme in Cardano. At the same time, we also have as a baseline to

	explore implementations of sharing mechanisms that enable rewards with relatively low variance, an issue that has been ignored in the current literature.
Team (Staffing)	Research Fellow (Incentives, Game Theory), 0.2 FTE (48 Months) Research Fellow (Allgorithm Design), 0.1 FTE (36 Months) Chief Scientist, 0.1 FTE (48 Months)

Global Identity

GI-1 Decentralized identity and reputation management

Research Lead: Jesus Diaz Vico
Start date: Jan 25
Duration (months): 48
2025 FTEs: 2
Intersect Product Roadmap: Programmable Assets

Objectives	(1) Work the foundations out, finalizing ongoing efforts, and extending them where needed (2) Look into ways to build those foundations (3) Look into the applications (4) Evaluate ways to integrate this global identity vision into existing stacks. Some of these main work packages may be done in parallel as they will likely inform each other.
Workplan	T1: Foundations (Start: M1, Duration: 15 months) Define the core properties of a global identity system—decentralization, interoperability, privacy, etc.—and explore foundational questions, including the role of PKI and credentials in this context. T2: Concrete Instantiations (Start: M6, Duration: 24 months) Assess whether current cryptographic tools are theoretically and practically sufficient to build a global identity system. Develop and evaluate concrete constructions using reference applications to validate real-world applicability. T3: Applications (Start: M25, Duration: 24 months) Identify blockchain-based (e.g., identity-enhanced governance, regulatory compliance) and traditional (e.g., web2 authentication) applications. Ensure selected use cases are supported by the constructions developed in T2. T4: Integration (Start: M12, Duration: 36 months) Evaluate integration pathways with existing stacks (e.g., Atala), aligning with current standards. Connect T2 outputs with T3 applications to ensure seamless adoption.

	This task focuses on innovation and tech transfer, essential to realizing a usable global identity system.
Deliverables	Research papers to be published at renowned security or cryptography conferences: D1. 2-3 research papers on Foundations D2. 1-3 research papers on Concrete Installations D3. 1-3 papers on Applications PoC-level libraries for benchmarking the proposed global identity solution: D4. 1 PoC per paper in Concrete Foundations (ideally, extra libraries with shared functionality) D5. PoC-level tools integrating the proposed systems into existing stacks (e.g., Atala). D6. 1 PoC per paper in Applications D7. Specifications extending existing standards (e.g. RFCs) to support the notion of global identity. This will depend on Concrete chosen technologies and their status at the moment of looking into integration and compatibility. Natural targets are W3C DIDs, W3C VCs, Hyperledger Anoncreds, and the RFCs they rely upon. Deliverables will be revised and refined as research progresses
Impact	Establishing the foundations of (decentralized) identity systems, and associated frameworks, such as PKIs. This domain has lacked formalization. This research will equip Cardano's broader ecosystem with the (theoretical, and PoC-level code) tooling to augment everything we do with identity-related information, in a privacy-preserving manner.
Minimal Requirements	Establish a formal notion of what a global identity is, and how it relates to current notions like decentralized identifiers (DIDs), Verifiable Credentials (VCs) and Anonymous Credentials (ACs). Augment Cardano’s core to be compatible with this global identity notion for its internal processes (transactions, smart contracts, governance).
Team (Staffing)	Research Engineer (Governance), 0.7 FTE (48 Months) Senior Research Fellow (Security), 0.1 FTE (48 Months) Senior Research Fellow (Layer 2), 0.1 FTE (48 Months) Research Fellow (Protocol Design / Security), 0.4 FTE (48 Months) Research Fellow (Programming Languages), 0.1 FTE (24 Months) Research Fellow (Cryptography), 0.1 FTE (24 Months) Cryptographic Engineer, 0.5 FTE (27 Months)

Democracy 4.0

D4-1: Next-level governance protocols

Research Lead: Raghav Bhaskar
Start date: Jan 24
Duration (months): 48
2025 FTEs: 1.2
Intersect Product Roadmap: Architectural Excellence

Objectives	Our goal is to develop a deep understanding of the requirements of a blockchain governance/voting protocol and develop a series of practical solutions that meet these requirements under formal security guarantees using different layer 2 protocols and cost.
Workplan	Phase 1 (24 months) D1. A paper on the trade-offs of security and cost when using various layer 2 primitives to lower the overall governance cost D2. A paper that brings out the benefits of using a blockchain for a governance protocol. D3. The developed security framework developed to study the security of the various protocols may itself be worth publishing. Phase 2 (24 months) D4. We will engage with the engineering teams that have requirements around governance/voting to deliver adapted versions of our governance protocols for their applications D5. (a,b) We expect phase two will result in another 1-2 papers on the broader governance questions.
Deliverables	Phase 1 T1. Design layer 2 voting protocols (Start: M1, Duration 4 months) T2. Develop a security model to analyze the security of voting protocols (Start: M1, Duration 8 months) T3. Validate the security and robustness of the developed protocols through an evidence-based methodology (Start: M5, Duration 6 months) T4. Evaluate and compare the security, performance and scalability of various governance and voting protocols (Start: M11, Duration 12 months) Phase 2 T5. Revisit the governance requirements in general blockchain systems and design governance protocols (Start: M25, Duration 24 months) T6. Engage with teams within Cardano interested in adapting any of the proposed governance protocols for their applications (Start: M25, Duration 24 months)

Impact	A desirable impact would be the use of one or more of these protocols for running elections/governance efforts more effectively within the Cardano ecosystem (eg. Catalyst/Cardano Foundation elections).
Minimal Requirements	We will develop a governance protocol that meets the requirements of Cardano's ecosystem in terms of security, layer 2 footprint and budget constraints. At minimum the solutions should allow for direct (non-delegated) voting, should offer vote privacy and end-to-end verifiability. The solution should also offer high degrees of censorship resistance.
Team (Staffing)	Research Fellow (Cryptography), 0.3 FTE (48 months) Research Fellow (Protocol Design / Security), 0.3 FTE (48 months) Research Fellow (Cryptography), 0.2 FTE (48 months) Senior Research Fellow (Consensus), 0.2 FTE (48 months) Chief Scientist, 0.1 FTE (48 months) Software engineer, 1 FTE (24 months)

D4-2: Governance incentives

Research Lead: Evangelos Markakis
Start date: Jan 23
Duration (months): 48
2025 FTEs: 0.8
Intersect Product Roadmap: Architectural Excellence

Objectives	The goal is to obtain a deeper understanding on the intricacies, the merits and the game-theoretic aspects regarding the design of voting procedures.
Workplan	T1. DRep reward schemes. (Start: M1, Duration: 30 months) T2. Weighted voting rules for the Voltaire era. (Start: M13, Duration: 24 months) T3. Voting rules for Participatory Budgeting. (Start: M18, Duration: 30 months)
Deliverables	D1. Paper on DRep incentives and reward schemes D2. Paper on Participatory Budgeting D3. Paper on governance centralization and civil attack risk
Impact	The outcome of this research is aimed at improving in the long term the current procedures that are in place for project Catalyst and at the same time the voting procedures for the governance actions during the Voltaire era. Both Voltaire and Catalyst are significant components for the entire Cardano community, and therefore it is of utmost importance to have well thought out election procedures that can reduce the risks and dangers arising from malicious users.

Minimal Requirements	1) A rigorous study of the DRep incentives and the proposal of appropriate reward schemes in the context of Voltaire. 2) A study and adaptation of recently proposed voting methods for Participatory Budgeting, such as the method of equal shares.
Team (Staffing)	Research Fellow (Incentives), 0.4 FTE (48 months) Research Fellow (Algorithms), 0.4 FTE (48 months)

The Internet Hydra-ted

IHT-1: Hydra Tail

Research Lead: Pooya Farshim
Start date: Jan 22
Duration (months): 36
2025 FTEs: 1.1
Intersect Product Roadmap: L2 Expansion

Objectives	The goal is to construct provably secure zk-rollup protocols with a view towards solutions that cater for Cardano's scalability needs.
Workplan	Main research thread (Start: M1, Duration: 24 months) T1. Define an appropriate UC functionality for zk-rollups (in a model where Cardano is a globally available blockchain) which satisfies the security properties expected in practice. T2. Design and analyze protocols with respect to the said security definitions tailored in particular to Cardano's UTxO-based ecosystem. Describe the on-chain and off-chain components of the system (see diagram below). Provide security proofs. T3. Study how cost-effective the solution is in terms of its mainchain footprint and other relevant measures such as (settlement) time or communication complexities. Additional research (Start: M25, Duration: 12 months) T4. Enabling off-chain smart contracts via isomorphism (where crypto primitives are appropriately translated). T5. The optimality of solutions with respect to various trust and economic assumptions. T6. Relations and commonalities with zk-bridges and layer-2 governance.
Deliverables	D1. A core research paper to be published at a leading security or cryptography conference. D2. Follow-up paper on a rollup solution that offers isomorphism.
Impact	By increasing the number of transactions processed per second at reduced fees, zk-rollup forms a core technology to support Cardano's scalability needs.

Minimal Requirements	The rollup protocols, at minimum, must offer an offchain pay-to-pub-key functionality to clients. It must guarantee security in the face of a malicious server that does not follow the protocol specification or attempt to censor/ignore users. At the same time, and in order to reduce operating costs, we target solutions that require no (or minimal) collateral from the rollup server.
Team (Staffing)	Research Fellow (Cryptography), 0.2 FTE (36 Months) Formal Methods Engineer, 0.2 FTE (36 Months) Research Fellow (Consensus), 0.2 FTE (36 Months) Research Fellow (Protocol Design/Security), 0.2 FTE (36 Months) Senior Research Fellow (Distributed Systems), 0.2 FTE (36 Months) Chief Scientist, 0.1 FTE (36 Months)

IHT-2: Inter-Head

Research Lead: Mario Larangeira
Start date: Jan 25
Duration (months): 60
2025 FTEs: 1.3
Intersect Product Roadmap: L2 Expansion

Objectives	This work aims to formally prove security of Hydra in the UC framework and lay groundwork for rigorous security proofs in the UC framework for any protocols relying on it.
Workplan	Objective 1: Research paper and proposal of the formalization of Hydra [1] in the UC framework. T1. Identification and formalization of the functionalities Hydra [1], consists of and relies on (Start: M1, Duration: 18 months) T2. Prove Hydra implements these functionalities which potentially requires adjustments to the Hydra protocol itself (Start: M1, Duration: 18 months) Objective 2: Research paper and proposal of the formalization of the Interhead Protocol [2] in the UC framework. T3. Investigation of components of Inter-Head Protocol [2], e.g., existing BFT protocols, and concrete parameters (Start: M19, Duration: 12 months) T4. UC formalization of the Inter-Head Protocol [2] keeping compactibility of the protocol developed in the earlier two tasks (Start: M19, Duration: 12 months) Objective 3: Universal Composition of the Optimization Tools Protocols, proposed in Research Plan: Optimization Tools, into the devised framework for UC Hydra and UC Interhead. T5. Investigation of concrete parameters for Hydra [1] / Inter-Head Protocol [2], i.e., collateral amount, time-locks, etc (Start: M31, Duration: 30 months) T6. Integrate Hydra optimization tools into the formalized UC versions of Hydra and

	Interhead (from earlier tasks) (Start: M31, Duration: 30 months)
Deliverables	D1. Research paper for Objective-1: Formalization of Hydra [1] in the UC framework. D2. Research paper for Objective-2: Formalization of the Interhead Protocol [2] in the UC framework. D3. Depending on the research resulting from IHT-3: Optimization Tools, at least three more papers for Objective 3: Universal Composition of the Optimization Tools Protocols, Integrate Hydra optimization tools into the devised framework for UC Hydra and UC Interhead.
Impact	This project is to determine the security of Hydra and Interhead while composing with other protocols to construct more complex applications. Layer-2 is one of the best approaches to increase the number of transactions. It can be used as the foundation for creating applications/protocols, acting as a middle ware to the consensus layer. In order to safely rely on such a design to safely compose with other applications, it is paramount to investigate the universal composability of Hydra and Interhead.
Minimal Requirements	Formalization of Hydra in the UC framework.
Team (Staffing)	Research Fellow (Cryptography), 0.4 FTE (60 Months) Research Fellow (Cryptography), 0.4 FTE (60 Months) UC Framework Expertise, 0.5 FTE (30 Months)

IHT-3: Optimization tools

Research Lead: Mario Larangeira
Start date: Jul 25
Duration (months): 60
2025 FTEs: 0.8
Intersect Product Roadmap: L2 Expansion

Objectives	To identify and develop critical tools/protocols to aid the smooth and safe operation of the Hydra suite Protocols.
Workplan	Objective 1: A survey/report paper for internal consumption: T1. Literature review: Which of the existing tool protocols in layer 2 are relevant for Hydra Suite of Protocols? (Start: M1, Duration: 12 months) T2. Literature review: Given all the relevant tool protocols, are they compatible with the Hydra Suite of protocols? (Start: M1, Duration: 12 months) Objective 2: A short list of identified problems/gaps, and protocols, along with its required tasks in order to make them Hydra compatible: T3. Do existing protocols for layer 2 need some adaptation to work in a Hydra based layer? (Start: M13, Duration: 6 months) T4. Is there any gap in the literature specifically for the Hydra Suite of protocol? Are

	there problems that do not exist in other layer 2 solutions, but are relevant for Hydra? (Start: M13, Duration: 6 months) Objective 3: Adaptation of existing protocols (in order to be used with Hydra) or creation of new ones. T5. Given the found compatibility, or not, which are necessary for further development? (Start: M19, Duration: 42 months) T6. The actual development of the proposed protocols. (Start: M19, Duration: 42 months)
Deliverables	D1. At least an internal report/survey mapping the current existing layer 2 protocols and its relevance/compatibility with Hydra Suite of Protocols. D2. A short list of protocols that fill gaps in the Hydra use cases along with existing protocols that exist but require development/adaptation in order to become Hydra compatible D3. The development/adaptation of the concrete protocols.
Impact	Similarly, to hydra and interhead which can be used as a foundation for more sophisticated application, therefore its universal composability needs to be thoroughly analyzed. In addition to the design with Hydra and interhead, more specific auxiliary protocols can also be used, hence they need their composability to be proven. The goal of this project is to establish the security of auxiliary protocols with respect to our base layer 2 protocols, Hydra and Interhead.
Minimal Requirements	The developed protocols must be compatible with any protocols in the Hydra suite.
Team (Staffing)	Research Fellow (Cryptography), 0.4 FTE (60 Months) Research Fellow (Cryptography), 0.4 FTE (60 Months)

IHT-4 Auditing tools

Research Lead: Christian Badertscher
Start date: Mar 23
Duration (months): 48
2025 FTEs: 2.8
Intersect Product Roadmap: L2 Expansion

Objectives	Hydra-Centric Prototype: Develop a practical, minimal-effort solution for auditability in Hydra. The outcome will be a research paper outlining a privacy-preserving and sound auditable protocol that exports relevant data to external auditors with basic identifiability features. General State-Channel Design: Build on T1 to define a formal, first-principles framework for auditable layer 2 protocols. Produce a generalized cryptographic state-channel construction suitable for integration with various blockchains.

	Compliance Groups: Introduce and define “compliance groups”—user groups governed by regulatory policies (e.g., FATF travel rule) enforced through cryptographic mechanisms. These groups operate with auditable, privacy-preserving execution, incorporating identity-based enrollment and revocation tools. Auditability as a Service: Extend the compliance layer beyond Cardano by designing an interoperable bridge for external, non-native entities to leverage Cardano’s compliance infrastructure. This enables compliant, auditable executions without requiring stake in Cardano.
Workplan	T1. How to define and formalize auditability, accountability, and privacy in the context of layer 2 protocols? (Start: M1, Duration 12 months) T2. What should an audit process for layer 2 protocols look like? (Start: M13, Duration 12 months) T3. Define, from first principles, all desired features that such a channel should support. (Start: M25, Duration 18 months) (1) interface with identity layers and external systems (2) how does it align with Rollup and ZK-technology as well as enhanced cryptographic functionalities to enable compliance and accountability (3) how it should bridge between different systems regarding enrolment and identification. T4. Come up with solutions that satisfy the identified needs and prove their security. (Start: M42, Duration 12 months)
Deliverables	D1. Hydra-Centric: (i) Design of a first solution fulfilling the minimal requirements laid out above. (ii) A research paper that describes an auditable Hydra protocol that exports information to an external auditor, while providing soundness and privacy, as well as a certain form of identifiability. D2. State-Channel Design: A research paper that presents a state-channel construction whose design is applicable to various layer 1 blockchains. D3. Compliance Groups: Realizing the vision of full-fledged policy-compliant execution as a layer 2 protocol, using cryptographic mechanisms to protect and prove the compliance of states to layer 1. D4. Auditability as a service: A research paper on providing auditability All papers would be supported with simulations and creating executable artifacts to inform future software development.
Impact	Accountability has become a key focus in recent years, with growing interest in privacy-preserving yet auditable systems, particularly at the layer 1 level and in CBDCs. This research elevates the concept to layer 2, enabling complex multi-party computations with integrated auditability using advanced cryptographic tools. The outcome will support scalable, privacy-preserving, and accountable execution—attractive to industry and financial institutions—and offer a compliance layer that external systems can access via interoperability with Cardano.

Minimal Requirements	The protocol must enable financial institutions to perform transaction-graph analysis based on the exported information from a Hydra state channel. At the same time, auditing an honest party should not result in obtaining more information than what parties agree when opening the channel. Any MVP must realize the idea of controlled exposure of information.
Team (Staffing)	Research Fellow (Layer 2), 0.2 FTE (48 Months) Research Fellow (Layer 2), 0.2 FTE (48 Months) Research Fellow (Privacy Preserving Technologies), 0.2 FTE (48 Months) Research Fellow (Privacy Preserving Technologies), 0.2 FTE (36 Months) 2 Postdocs, 0.5 FTE (24 months) 1 PhD, 0.5 FTE (12 months) Engineer, 1 FTE (36 months)

Interchains

IC-3: Light client infrastructure

Research Lead: Marc Roeschlin
Start date: Jul 23
Duration (months): 48
2025 FTEs: 1.5
Intersect Product Roadmap: Developer / User Experience, Architectural Excellence

Objectives	Develop a secure light client protocol that enables wallet functionality and basic smart contract interactions with minimal reliance on external resources or trust. Long-Term Vision: As blockchain data grows, full-chain storage will become impractical, with a few actors maintaining archives and likely charging for access. Existing services like Blockfrost highlight this, though their proprietary interfaces introduce third-party trust issues. This research aims to define standardized, secure access methods as part of the blockchain ecosystem. If needed, supporting query and notification mechanisms will be designed to help light clients operate without full chain access. All components will be built with composability and formal security proofs to ensure robust, seamless integration.
Workplan	Research paper(s) to be published at renowned security or cryptography venues. D1. One paper for light client protocol (18 months, Q4 24) D2. One paper on formalization (12 months, Q4 25) D3. One paper covering extensions (18 months, Q2 27). Publishable units schedule to be reconfirmed and defined.

Deliverables	T1. Envision three possible research directions that introduce novelty in the light client space.(Start: M1, Duration: 48 months). T2. Analyze how smart contracts interact with the blockchain and then define the requirements for a light client in terms of expected functionality. (Start: M1, Duration: 12 Months). T3. Analyze and construct the light client protocol from first principles (Start: M1, Duration: 12 Months). T4. Define and formalize the functionality of light client(s) (Start: M18, Duration: 18 Months). T5. What data should a checkpoint include to help a light client find past transactions, addresses, and handle new transactions while waiting for the next checkpoint? (Start: M1, Duration: 36 Months). T6. Analyze trade-offs and propose a light client infrastructure that supports various use cases, including DApp development and mobile wallets. The main KPIs for light clients will focus on security guarantees and performance improvements over full node operation. (Start: M37, Duration: 12 Months) T7. Analyze privacy considerations based on the design of the light client infrastructure. (Start: M37, Duration: 12 Months)
Impact	Resources to monitor a blockchain and construct proofs are growing at an alarming rate. Light clients are needed for wallets, Dapps, etc.
Minimal Requirements	The light client protocol must implement a functionality that allows the obtaining and verification of ledger state and the history of the chain, as well as, emit transactions. Additionally, it needs to be able to engage in (and possibly create/submit) “simpler” smart contracts.
Team (Staffing)	Research Fellow (Formal Methods and Verification), 0.4 FTE (48 months) Research Fellow (Distributed Systems), 0.4 FTE (48 months) Research Fellow (Consensus, Applied Cryptography), 0.2 FTE (48 months) Chief Scientist, 0.1 FTE (48 months) 1-2 Further Researchers (Consensus + Distributed Systems): 0.4 FTE (48 months)

IC-4.1: DApp Tokenomics

Research Lead: Paolo Penna
Start date: Jan 25
Duration (months): 24
2025 FTEs: 1.6
Intersect Product Roadmap: Programmable Assets

Objectives	Investigate and compare a number of practical solutions currently implemented by Cardano and other systems, and their main differences, advantageous, and potential weaknesses.

Workplan	T1. How can/should the DApps, systems or partnerchains reward contributors with tokens from this new system? (Start: M1, Duration 12 Months) T2. How long should the launch phase persist, and what events (if any) should trigger the start of normal operation? (Start: M1, Duration 12 Months) T3. What form of investment can the DApp, system or partnerchain designer implement to maximize its success while staying within a reasonable budget? (Start: M7, Duration 12 Months) T4. Under what conditions is it beneficial for both parties (mainchain and DApp / new system) to engage and collaborate during the launching phase? (Start: M13, Duration 12 Months)
Deliverables	This research stream is expected to first produce research papers targeting top-tier conferences. D1. Modeling tokenomics design and the “convergence” to a desired target state at the end of the launching phase D2. What investments and strategies the designer can put in place to accelerate and improve the chances of “success” of the launching phase, in particular, the benefits of a mainchain paradigm. D3/D4. Depending on the findings, further research will focus on the minimal technological functionalities (e.g., limited bridge, tokens’ minimal interoperability, etc.) necessary in the first place. This is expected to produce at least two more publications.
Impact	Economic, adoption and ecosystem growth, more diverse and broader tokenomics capabilities.
Minimal Requirements	The new mathematical models developed with this research shall incorporate (i) metrics to quantify the “success” of a new application, system or integration after some finite “launching phase”, (ii) the key parameters that mostly impact on the success, e.g. the initial investment and resources offered by the mainchain, (iii) how the mainchain (e.g., Cardano) and its ecosystem can benefit in terms of tokenomics policies and economic stability.
Team (Staffing)	Research Fellow (Game Theory / Economics), 0.5 FTE (24 Months) Research Fellow (Game Theory / Economics), 0.5 FTE (24 Months) Research Fellow (Game Theory / Economics), 0.5 FTE (24 Months) Chief Scientist, 0.1 FTE (24 Months)

IC-4.2: Consensus Innovation

Research Lead: Christian Badertscher
Start date: Sep 24
Duration (months): 54
2025 FTEs: 1.8
Intersect Product Roadmap: Architectural Excellence

Objectives	Basic expectations. This research stream shall propose at least three distinct set of solutions: 1. It investigates and assists the development effort on competitive algorithms for the partner chains framework. 2. It shows how the consensus layer of Cardano could be strengthened beyond the synchronous model of execution. 3. It develops DAG-based protocols in the dynamic participation and permissionless PoS setting and informs other research streams about improvements based on new consensus paradigms. Core Questions. To meet the basic expectation, the following questions are relevant: 1. How can the synchronous model of execution of Ouroboors be relaxed, e.g. by adjusting the active-slot coefficient adaptively? 2. How can we achieve faster block rates based on adaptivity of the active-slot coefficient? 3. What are the crucial aspects of DAG based protocols that we can replicate in a true permissionless framework under dynamic participation? How could Mithril assist in achieving such a DAG based protocol?
Workplan	T1: Applied Research for provably secure iterated BFT protocols (Start: M1, Duration: 12 months) T2 - Non-synchronous blockchains (Start: M13, Duration: 15 months) T3 - DAG based approaches in the dynamic participation world (Start: M26, Duration: 15 months) T4 - New features, stronger guarantees, incentives (Start: M42, Duration: 12 months)
Deliverables	D1. Applied Research for provably secure iterated BFT protocols D2. The design of a mechanism for Ouroboros to change the active-slot coefficient adaptively, together with rigorous security proofs and assisted by formal methods tools. D3. A secure DAG-based PoS protocol offering best in class security and efficiency. D4. A paper on the design of a novel, robust consensus algorithm that proves enhanced security and incentive properties. All papers would be supported with simulations and creating executable artifacts to inform future software development.
Impact	For the long-term objective, the research can yield new types of consensus algorithms relevant for the future of Cardano backbone itself.
Minimal Requirements	n/a
Team (Staffing)	Research Fellow (Consensus Research), 0.3 FTE (54 Months) Research Fellow (Consensus Research), 0.3 FTE (54 Months) Research Fellow (Consensus Research), 0.2 FTE (54 Months) Research Fellow (Consensus Research), 0.2 FTE (54 Months) Formal Methods Engineer, 0.2 FTE (12 months)

	Research Associate, 0.25 FTE (42 months) Research Associate, 0.25 FTE (27 months) Chief Scientist, 0.1 FT (54 months)

3.4 Technology Validation Workstreams

Technology Validation workstreams serve as a critical bridge between foundational research and real-world implementation, enabling the Cardano ecosystem to transform cutting-edge concepts into viable, high-impact solutions. These workstreams are structured to rapidly test, refine, and validate research opportunities through hands-on prototyping and cross-functional collaboration. By navigating streams from SRL2 through to SRL4/5, they provide clear proof points that de-risk further investment and set the stage for broader adoption.

A key strength of this approach is its emphasis on accelerated development. Rapid prototyping enables faster iteration cycles, turning theoretical designs into tangible outputs in a short timeframe. This not only reduces time-to-value but also allows teams to pivot early in response to new findings. Through early testing and validation, potential technical or conceptual weaknesses are identified and addressed before significant resources are committed—substantially mitigating risk and improving resource efficiency.

These workstreams also promote enhanced collaboration among researchers, engineers, cryptographers, formal method experts, and product teams. This multidisciplinary model ensures that innovations are tested within realistic parameters. Prototypes produced during this phase serve as both functional demonstrations and collaboration tools, offering stakeholders clear evidence of progress and increasing confidence in the technology's direction. They also support market alignment, with early versions providing a basis for user feedback and customer testing, helping to validate commercial potential.

Workstreams are internally supported by engineering, product, and research leads and are aligned through a structured Intersect process. Each proposal is reviewed and approved in batches by the Product Committee, ensuring strategic coherence and resource prioritization. This process socializes proposed research opportunities with key community stakeholders, informs scaling strategies, and ultimately strengthens the Cardano ecosystem by fostering a culture of continuous improvement and commercial readiness.

TV-1. Leios

Workstream Lead: William Wolf
Start Date: Sept 24
Duration (months): 12
Target SRL: 4
Target BRL: 4
2025 FTEs: 7.75
Intersect Working Group: Consensus
Intersect Product Roadmap: Leios

Ouroboros Leios is a high-throughput protocol for Cardano. It is designed to maximise the use of available network bandwidth and therefore maximise overall throughput of the network, all while maintaining the strong security properties of the Ouroboros family of protocols. Being agnostic of the underlying Nakomoto consensus protocol, Ouroboros Leios can support a wide range of applications. This innovation workstream for Leios aims to evaluate the protocol's viability for practical use and to advance the protocol's maturity from the research stage to a stage where development for eventual deployment can begin.

Problem: As Cardano evolves, there will be increasing demand for greater network capacity to support new and existing users and applications. Ouroboros Praos, being a serial protocol based on Nakamoto consensus, has stringent practical limitations on the number of transactions its blocks can contain and the speed at which new blocks can be produced. There are significant opportunities to scale: the network and CPU resources on most nodes are almost idle much of the time. With a different algorithm, these resources can be used to increase the total chain bandwidth. In order to substantially scale beyond this necessitates changes to the underlying blockchain algorithm. A more parallel protocol is required to optimally utilise available network bandwidth and to increase the transaction rate supported by Cardano. This needs to be done without compromising security or slowing down settlement.

Innovation: Ouroboros Leios is designed specifically for scaling Cardano to high throughput, without compromising security. It introduces the concept of input blocks that are cryptographically pre-processed by input endorsers; those blocks are referenced in endorser blocks that are voted upon for inclusion by reference in the blocks of the base layer. The introduction of this hierarchy of block references to transactions enables a degree of parallelism that nearly optimally employs network resources. Verifiable random functions are used to select the parties that perform the necessary operations in parallel pipelines. The protocol and those pipelines are designed to maintain the level of security and performance guaranteed by the base protocol. Ouroboros Leios will meet expected future demands, providing a basis for continuing Cardano growth and scalability.

KPIs: (i) Maximum throughput attainable by Leios: analyse Leios simulations to determine the transaction throughput that is achievable under real-world network conditions. In theory Leios can target a 5x improvement throughput, at the cost of using 85% of available network bandwidth
(ii) Transaction lifecycle settlement time: quantify how Leios would affect the time from a transaction entering the memory pool of a node to its receiving one confirmation in a block of the base protocol.
(iii) Operating cost of a stakepool node: estimate the incremental cost of operating a block-producing node under Leios, as compared to Praos, and the potential impact this might have on the operators' ecosystem
(iv) Resilience to infrastructure disruption: quantify the robustness of Leios in terms of degradation of throughput and settlement time in the presence of numerous nodes going offline or losing network connectivity.
(v) Performance under attack: differentiate Leios from Praos under adversarial stake or network conditions.

Application Area: Implement multi-node simulations that are formally verified to be faithful to the Leios protocol. Develop analysis and visualisation tools to quantify Leios behaviour and performance.

Non-Functional Requirements: Simulations can be used interactively by the stakeholder community to

study Leios.

Business Model: The Leios innovation workstream lays the foundation for full development and deployment of Leios on Cardano. The primary artefacts support both the technical and business cases for that follow-on work. The innovation effort will liaise with external stakeholders (Intersect working groups and special interest groups) so that their questions and concerns regarding Leios are addressed by modelling, simulation, and analysis. The largest barrier is the need to demonstrate that Leios solves throughput-scaling for Cardano in a cost-effective manner, without disproportionately increasing the cost of operating stake pools. Leios's Protocol and ledger changes will also cascade into Cardano tooling, framework, and infrastructure. Solid technical analyses will lower these barriers by proposing designs that alleviate such concerns.

Scope	The overarching goal of this innovation project is to demonstrate the viability of implementing the Leios protocol on Cardano, as described in the associated research paper. To achieve this, we define the following objectives: ● Provide solid evidence supporting the practical applicability of the theoretical protocol. ● Develop an Agda specification that formally defines Leios. ● Conduct modeling, simulation, and analysis to quantify Leios' performance in relation to the goals explicitly outlined in the research paper and related documentation. ● Define and model the protocol's security properties, and formalize the underlying cryptographic components. ● Clarify the different variants ("flavours") of Leios—such as blob, short-pipeline, simplified, and full—and articulate their respective properties. ● Provide evidence that the Leios protocol addresses known limitations in Cardano's network throughput. ● Identify potential business cases for each Leios variant, propose deployment sequences, and collaborate with the product team to engage the Cardano community. ● Investigate related concerns and requirements raised by innovation, research, networking, consensus, ledger, and node teams, as well as special interest groups and other stakeholders. ● Deliver long-lived artifacts—such as simulators and conformance tests—only where there is strong evidence of ongoing utility beyond the innovation/prototyping phase. These tasks may be required to support specifying Leios as a Cardano Improvement Proposal (CIP). This effort assumes that the innovation and prototyping work has advanced Leios to at least Software Readiness Level 4 (SRL4). It also includes supporting the hand-off process to Intersect. The project is assumed to have "graduated" to the CIP phase (e.g., SRL4) and to be

	ready for further development. Advancement to SRL5 or SRL6 should occur only if the term “relevant environment” is clearly and narrowly defined. The overarching goal of the innovation project is to demonstrate the viability of implementing on Cardano the Leios protocol as described in the research paper.
Workplan	12-Month Work Plan Including Handover to Intersect: The objective of this work plan is to advance the Leios protocol through a focused innovation phase, culminating in a smooth handover to the implementation team at Intersect. The work is expected to conclude by summer 2025, aligning with the implementation team’s readiness to begin development. T1. Agda Formal and Executable Specification: Develop a formal specification of the Leios protocol in Agda, ensuring it is both mathematically rigorous and executable for validation purposes. T2. Protocol Simulation and Adversarial Analysis (i) Develop a detailed simulator or animated visualisation of the Leios protocol for a small set of nodes. (ii) Define and simulate adversarial behaviours at the protocol level that could impact performance or correctness, including denial of service (DoS), block duplication, vote equivocation, adversarial certificates, and private chains. (iii) Merge the existing nascent simulators into a unified, possibly modular, simulation framework. T3. Conformance Tests: Develop and validate conformance tests to ensure that future implementations of Leios adhere to the protocol specification. T4. Large-Scale Network Simulator: Build a coarse-grained, scalable network simulator capable of modelling Leios at the scale of the Cardano network. This simulator should estimate protocol impact on network and node resources. It may draw inspiration from tools like PeerNet, with a focus on improved usability for broader adoption. T5. DeltaQ Analysis: Conduct a DeltaQ-style analysis to quantify the quality of service and performance characteristics of Leios under a variety of conditions, including normal and degraded network environments.
Dependencies	Leios, Anti-grinding and Mithril may all be interdependent
Deliverables	D1. Web-based simulators: (i) Protocol and network simulator for various flavours (ii) Performance dashboards (eg. analysis of various properties and characteristics related to the protocol under varying parameters) D2. Quarterly incremental technical report(s) D3. Protocol behaviour analysis under various scenarios D4. CIP D5. Conformance tests

Innovation Goal	Technical analyses, Prototype simulations, Conformance tests, Formal specs
Team	Product Manager, 0.35 FTE, 12 months Technical Architect, 1.00 FTE, 12 months Prototyping/Software Engineers, 3.3 FTE, 12 months Applied Cryptographer, 0.5 FTE, 12 months Formal Methods Engineer, 1.5 FTE, 12 months Developer Relations 0.5 FTE, 9 months Project Manager 0.3 FTE, 12 months
Documentation	[1] High-Throughput Blockchain Consensus under Realistic Network Assumptions [2] Ouroboros Leios: design goals and concepts [3] 'Near optimal throughput': A deep dive into Ouroboros Leios [4] Scaling blockchain protocols: a research-based approach [5] https://leios.cardano-scaling.org/ [6] CIP-0079? | Implement Ouroboros Leios to increase Cardano throughput cardano-foundation/CIPs#379

TV-2. Anti-grinding

Workstream Lead: Nicolas Henin
Start Date: Oct 24
Duration (months): 9
Target SRL: 4
Target BRL: 4
2025 FTEs: 4.15
Intersect Working Group: Consensus
Intersect Product Roadmap: Architectural Excellence

Theoretical estimates of settlement times on the Cardano mainchain are heavily influenced by the potential impact of a “grinding attack.” To mitigate this effect and enable faster settlement, this stream focuses on evaluating protocol changes that significantly increase the cost of executing such attacks. By raising the computational expense required, the protocol constrains adversaries—regardless of their available computational power—forcing them to resort to much weaker and less effective forms of the attack.

Problem: The Praos consensus protocol—a key component of the Ouroboros family—secures blockchain networks through the use of verifiable randomness in slot leader elections. However, it is susceptible to a grinding attack, in which an adversary systematically explores potential inputs to manipulate or predict the randomness used in leader selection. This increases the attacker’s chances of being elected as a slot leader, undermining the fairness and security of the protocol. This vulnerability impacts not only the network’s security but also its performance, particularly settlement times. By

influencing the leader selection process, an attacker can delay or manipulate block production, resulting in slower transaction settlement. The challenge lies in strengthening the randomness generation mechanism in Praos to prevent such exploitation, while simultaneously improving protocol efficiency to ensure fast and reliable transaction finality.

Innovation: The overarching objective of this work is to achieve faster settlement times on the Cardano network. The proposed approach focuses on strengthening anti-grinding measures within the Praos protocol. The core challenge lies in enhancing the randomness generation mechanism in Praos to prevent adversarial exploitation, while simultaneously improving protocol efficiency to support fast and reliable transaction settlement. In the security analysis of Ouroboros Praos, the grinding attack threat is mitigated by estimating the computational cost of a single grinding attempt. By assuming an upper bound on the adversary's computational power during the narrow time window in which grinding must occur, the number of feasible attempts is capped. The protocol is then carefully parameterized—particularly in terms of settlement time—to ensure security even in the presence of this limited grinding capability. The key idea behind the proposed protocol enhancement is to significantly increase the cost of a single grinding attempt. By doing so, the number of attempts an adversary can carry out within a given computational budget is reduced, thereby limiting their ability to influence slot leader selection and improving overall settlement performance.

KPIs: Reduction of the parameter k
(i) 10^11-fold increase in the complexity of a single grinding attempt, as measured in commodity-CPU work.
(ii) Improves substantially settlement times under grinding attack. (N.B quantification available in Quick Wins for Cardano Settlement)

Application Area: (i) New Incremental η (eta) Cryptographic Function over a R window (Production Ready Level - Implementation/Formalisation/Benchmark). (ii) Updated Agda specification for the consensus.

Non-Functional Requirements:

- Performance: The Node Hardware Architecture should be minimally impacted.
- Scalability: Should not be impacted
- Security: Security improved regarding grinding attacks.
- Maintainability: Work should be detailed enough to minimally challenge the specification and the
- design while integrating the proposal. (seamless flow of work)
- Interoperability: The Proposal sustainability should be clearly expressed, how compatible this proposal will be with future Ouroboros versions (Praos, Genesis, Peras, Leios etc...)
- Compliance: Should be Formally Specified with an updated Agda Specification

Market: Anti-grinding implementation will have the following outcome: (1) Mitigate the progress of hardware computation since the launch of Cardano when it comes to grinding-attack. (2) Go beyond this level, to increase the settlement probability of Carddano Faster settlement is important for any cross-chain operations and for risk assessment of dApps.

Business model: Anti-grinding is already a feature of the existing Cardano Ouroboros consensus protocol. The go-to-market strategy focuses on demonstrating two key benefits: (1) a quantifiable increase in security against grinding attacks, and (2) a measurable reduction in the required k parameter,

which directly contributes to faster settlement times. The primary barrier to adoption is the potential perception among Intersect and the broader Cardano community that the grinding attack vector is either not sufficiently relevant or does not offer a strong return on investment relative to its perceived risk. This could lead to a decision not to proceed with implementation, despite the technical merits.

Scope	A preliminary effort has been made to validate two independent improvements: 1. Strengthening the anti-grinding measures in Praos 2. Optimizing the Block-Creation rate by just changing the Active Slot Coefficient "f" The scope of this initiative is to focus on the first improvement and provide details of implementation for an eventual integration in Ouroboros-consensus: **Consolidated Specification Document** (i)Value Proposition: Quantify the added Security against Grinding Attacks, Quantify the “parameter k” reduction (ii) Sustainability of the proposal: Application on Praos, Genesis, Peras, Leios Out of Scope: The implementation of the integration per se (this is under the responsibility of Consensus teams)
Workplan	T1. Rationale for the Selection of the Chosen Primitive Among Alternatives T2. Specification of the solution T3. Prototype containing the proposed Implementation, including Testing and benchmarks T4. Submission of CPS T5. Submission of CIP
Dependencies	n/a
Deliverables	D1. Documents: (i) Specification (ii) Solution Proposal (iii) CIP D2. Software: (i) New Incremental η (eta) Cryptographic Function over a R window (Production Ready Level - Implementation/Formalisation/Benchmark), (ii) Updated Agda specification for the consensus
Innovation Goal	Ease the integration (by the Intersect Consensus Team) of this improvement: 1. Specification 2. Technical Design: (i) Technical analyses (ii) Impact analyses 3. Formal Specification
Team	Product Manager, 0.35 FTE, 6 months Technical Architect, 1 FTE, 6 months Prototyping/Software Engineer, 1 FTE, 6 months Applied Cryptographer, 0.5 FTE, 6 months Formal Methods Engineer, 1 FTE, 6 months Developer Relations 0.3 FTE, 6 months
Documentation	Leios documentation, and its impact on block production rate

TV-3. Jolteon Liveness

Workstream Lead: Dominik Zajkowski
Start Date: May 25
Duration (months): 6 *
Target SRL: 4
Target BRL: n/a
2025 FTEs: 3.4
Intersect Working Group: Consensus
Intersect Product Roadmap: Architectural Excellence

Jolteon has been selected as the consensus algorithm for PartnerChains (PC). The aim of this workstream is to provide engineering-based evidence that the Jolteon consensus protocol satisfies the liveness property.

Problem: The identified need is to establish clear conditions under which Jolteon can reliably preserve liveness. Chain stalls and reliance on centralized recovery mechanisms pose significant reputational risks for any PartnerChain implementation. Formal liveness proofs are essential to ensure that risk mitigations are both appropriate and effective. PartnerChains aims to enhance its security posture and reduce reputational exposure through the adoption of FastBFT, supported by formally validated specifications and, where feasible, verified implementations.

I**nnovation:** Jolteon liveness property has never been formally verified by another chain that is using Jolteon or a variant of it (Concordium, Aptos).

KPIs n/a

Functional Requirements (Application) Mechanized proof of liveness (have certainty under what conditions Jolteon is able to preserve liveness).

Non-Functional Requirements n/a

Market: Intersect, Partner Chains, Companies that base their clients on Jolteon (e.g. Aptos)

Business model: Mitigate the reputational risk of a potential crash of a Partnerchain if Grandpa+Aura fail the advertised safety and liveness properties. We cannot safely assume Grandpa meets its advertised safety or liveness guarantees. FastBFT is our best hope of replacing our Grandpa+Aura consensus with something we can actually trust.

Scope	After the mechanized safety proof has been developed as part of fastBFT, the next step is to mechanize the proof of liveness. Two angles to the solution: Mechanized liveness proof in Agda OR a clear statement why it's not feasible. Conformance platform: property tests trace based behavioral testing
Workplan *	T1. Feasibility to build a liveness proof T2. If feasible, build a mechanized proof T3. Improve the conformance platform property test coverage, incorporating the liveness proof findings T4. Build out trace based behavior verification
Dependencies	None
Deliverables *	D1. Documents: (i) Mechanized liveness proof (ii) Update plan to the relevant prototype D2. Software: (i) Conformance platform updates that incorporate liveness proof findings
Innovation goal	The identified need is to gain certainty under what conditions Jolteon is able to preserve liveness.
Team	Senior Architect 0.3 FTE Researcher 0.1 FTE Senior Formal Methods Engineer 2 FTE Prototyping/Simulation Engineer 1 FTE
Documentation	1. Formal Methods specialists: Jolteon Agda model, Streamlet Agda model, Jolteon mechanized proof of safety 2.Creative Engineering and Partnerchains Engineering for the Jolteon Substrate PoC. 3. Architecture to document the effort and provide evidence building the case for Software Readiness Level 4. 4. PoC integration of Jolteon into Substate.

* At the time of publication, workstream planning is still in progress and subject to change.

TV-4. RSnarks

Workstream Lead: Dmytro Kaidalov
Start Date: Feb 24
Duration (months): 15
Target SRL: 6
Target BRL: 1

2025 FTEs: 5.3
Intersect Working Group: Smart Contract
Intersect Product Roadmap: Developer / User Experience

This stream focuses on recursive SNARKs, which enable iterative aggregation of multiple proofs into a single, succinct proof, broadening the range of applications for privacy and scalability. A key application is the efficient proving of state progression in blockchain systems, such as enabling a trustless zk-bridge between Cardano and partnerchains. To achieve this, the workstream adapts the Halo2 proving system, utilizing Pluto-Eris curves and KZG commitments for smaller proofs and faster verification. The current focus is the translation of Halo2-Pluto proofs into Halo2-BLS proofs, which can be efficiently verified on Cardano. This involves complex recursive arithmetic and smart contract development, aiming to demonstrate feasibility and scalability of these innovations for blockchain ecosystems.

Problem: How can we efficiently perform recursive aggregation of SNARK proofs within the constraints of Cardano's Plutus platform, particularly for enabling a trustless zk-bridge between Cardano and partnerchains:

There are a number of business opportunities related to ZK technology in general, SNARK technology in particular and RSNARKs specifically. Since RSNARKs are in turn SNARKs and ZK tech, there is a hierarchy of opportunities that could be pursued in the space more broadly and as it pertains primarily to RNSARKs.

ZK tech broadly: There are a number of ZK technologies with different proving systems and curves which yield very different trade offs for the same basic concept: that of being able to convince a verifier of something, without revealing what that thing is.

SNARKs: The key characteristic of SNARKs is their succinctness, meaning that there is no challenging back and forth between the prover and verifier, instead the system relies on a trusted setup and the verifier is able to verify the proof without communication between the two parties.

RSNARKs: Recursive SNARKs are different from regular SNARKs in that the proof generation process involves the verification of one or more previous proofs.

Innovation: Cross-Curve Proof Translation: Translating proofs from Halo2-Pluto to Halo2-BLS, which involves performing complex in-circuit arithmetic across different elliptic curve fields—a process known as wrong-field arithmetic.

Computational Feasibility: Ensuring that the translation process remains efficient and feasible for provers, while also being compatible with Plutus smart contracts for on-chain verification.

Scalability Trade-offs: Carefully balancing trade-offs between proof size, verification time, and recursive scalability, to ensure the solution remains practical and performant within the constraints of Cardano’s blockchain infrastructure.

KPIs: (i) Enable on chain verification of Halo 2 proofs. (ii) Demonstrate that a proof can be split into several transactions if needed. (iii) Verify Halo2-BLS recursive proof in Plutus.

Application Area: Work with Halo 2 proofs

Non-Functional Requirements: A small proof should be verifiable within a transaction budget

Market: The market for RSNARKS-based technologies—particularly recursive SNARKs and the zk-bridge solution—spans several high-impact sectors within the blockchain and cryptocurrency ecosystem:

Blockchain Interoperability: The primary market includes projects focused on cross-chain communication and interoperability. A trustless zk-bridge, enabling secure data and asset exchange between blockchains (e.g., Cardano and PartnerChains such as Midnight), is a highly valuable component for ecosystems aiming to bridge currently siloed networks.

Scalable Blockchain Systems: As blockchain platforms like Cardano scale, recursive SNARKs offer a critical advantage by reducing proof and data sizes. This results in faster transaction processing and lower operational costs, making the technology attractive to any system prioritizing throughput, cost-efficiency, and sustainability.

Privacy-Focused Blockchain Applications; Projects with a strong emphasis on privacy—particularly in sectors like decentralized finance (DeFi) and data-sensitive applications—can use recursive SNARKs to verify transactions and state transitions without exposing underlying data. This enables highly scalable and secure privacy-preserving protocols.

Business Model: n/a

Scope	This workstream specifically focuses on the final translation step from Halo2-Pluto proofs to Halo2-BLS proofs. This includes: • Developing a Halo2-BLS recursive prover that can efficiently re-prove the Halo2-Pluto proof. • Creating a Halo2-BLS verifier that can operate within the constraints of a Plutus smart contract on Cardano. • Addressing the complexities of performing wrong-field arithmetic required for translating proofs between the Pluto curve and the BLS12-381 curve. • Assessing the feasibility and computational costs of this translation process and the verifier implementation on Cardano. • This work aims to ensure the scalability and practicality of recursive SNARKs for Cardano and beyond.
Workplan	T1. A technical report on recursive proof aggregation process T2. CIP for the MSM operations and simulations of its costs T3. Formally proving security properties of the foreign-field arithmetic algorithms developed by the Midnight team T4. Prototype of the Halo2 verifier in Plutus for recursive Halo2-BLS proof T5. Prototype splitting Halo2 Plutus verifier into several transactions on Cardano T6. Prototype Halo2-BLS circuit for the pairing check over a foreign elliptic curve
Dependencies	Halo 2 state aggregator

Deliverables	D1. Documents: (i) Prototype for the prover and the verifier (ii) CIP for the MSM operations D2. Software: Working prototype
Innovation goal	Proof of Concept on Mainnet
Team	Technical Architect, 1.25 FTE, 15 months Prototyping/Software Engineer, 1.25 FTE, 15 months Formal Methods Engineer, 1.25 FTE, 15 months Applied Cryptographer, 1.5 FTE, 15 months
Documentation	n/a

TV-5. Proof of Restake

Workstream Lead: Alex Slesarenko
Start Date: Feb 24
Duration (months): 19
Target SRL: 6
Target BRL: 1
2025 FTEs: 3.3
Intersect Working Group: Partnerchains, Consensus
Intersect Product Roadmap: L2 Expansion

Hybrid consensus systems combine two or more different consensus algorithms to leverage their strengths and mitigate their weaknesses. This approach enables the creation of a more robust, scalable, and secure consensus mechanism.

The Minotaur project aims to provide tooling for bootstrapping a new Proof-of-Stake (PoS) blockchains called Minotaur Chains. The primary challenge is the initial lack of stake distribution, which poses a security risk for a new chain. To address this, the project proposes leveraging existing stakes from established chains like Cardano and Ethereum to create a "Virtual Stake" on the Minotaur chain. This allows initial participants to secure the Minotaur network using their existing stakes on these chains.

The solution involves a dynamic conversion rate between the actual stakes on Cardano, Ethereum, and Minotaur, based on USD price oracles. The Virtual Stake is also defined by a list of weights for each chain. Validators from Cardano and Ethereum can register their participation on the Minotaur chain using their existing stakes (process called re-staking) and engage with smart contracts on Cardano and Ethereum, ensuring the initial security of the Minotaur network. Over time, as Minotaur coins are minted and staked, the Virtual Stake will gradually shift to prioritize Minotaur stakes.

Problem: Mapping Epochs: How can we relax the “alignment” requirement (of Ariadne) between the different epochs? How should we map the different times?

Stake Authentication: How can we connect an address on a main chain with the address on PC
How to penalise misbehaviour?

Finality Delay: How do we compensate for the potentially large time difference between the current PC slot and the most recent StakeDistribution snapshot obtained from other chains?

Cross-chain Transactions: The initial goal of Minotaur is to secure another blockchain, but it should be able to cover other scenarios, such as the management of cross-chain transactions.

DParameter Governance: In PC v1 DParameter is defined by smart contracts on Cardano (called Mainchain) and extracted via Mainchain Follower. In addition ETH resource into virtual stake we need to extend DParameter with additional number of ETH participants (in addition to ADA participants).

Innovation: Minotaur consensus may well be how new PoS blockchains are started going forward. The protocol allows new networks to bootstrap consensus using re-staked PoS tokens from already established networks. These are tokens with lower volatility, deeper liquidity and easy access, such as ETH.

KPIs: Evaluate 5 light clients solutions for ETH & Cardano

Application Area: Should provide an integration to the Partnerchains framework

Non-Functional Requirements: A committee selection is based on a stake aggregation of different resources.The first deliverable is a hardcoded dual staking approach using ADA and ETH. We would then focus on a more general approach that can deal with a mix of different resources chosen by the partnerchain.

On-chain contracts: (i) A set of contracts on Cardano to manage re-staking of ADA, e.g. quantities, slashing, etc. (ii) A set of contracts on Ethereum to manage re-staking of ETH and associated administrative tasks such as slashing.

Consensus processes: A process which stakers must run to partake in Partnerchain consensus. This process will compute the virtual stake based upon the re-staked resources from other networks and perform committee selection.

This is analogous to developing an Eigenlayer AVS and Cardano equivalent.

Market: Multi resource staking is a key element for creating DAOs and Partnerchains that operate cross network. It offers different entities a means to set up an operation model that depends on the resource they bring, independently of the chain on which they operate. Minotaur is also a huge opportunity for assets holders to restake their assets and be rewarded for that.

Business Model: Proof of restake provides a new revenue stream for SPOs and allows DAO and users of the partnerchains framework to borrow securities from Cardano and other chains. As it requires to

observe Cardano, it promotes an integration of the chain/organisation that uses proof of restake within the Cardano ecosystem.

Scope	The scope is limited to determining technical requirements and formal verification of the Minotaur consensus protocol.
Workplan	T1. Define a Minotaur protocol specification T2. Comparative analysis of different light clients for ETH and Cardano T3 Analyze potential usage of ETH restaking solutions, like Eigen Layer T4 .Perform simulation of protocol behaviour in response to events and potential attacks scenarios
Dependencies	None
Deliverables	D1. An algorithm for multi-resource slot leader selection D2. Proof of concept of the restaking mechanism on Cardano D3. Proof of concept of the restaking mechanism on Ethereum using Eigenlayer
Innovation goal	Smart contract for restaking outside of Cardano and observation on Minotaur. - Enable aggregation of multiple resources (different Cardano native assets or other L1 tokens) to secure a proof of stake algorithm. - The objective is the definition of a slot leader selection based on the restake of different participants to Minotaur; it enables fair selection of a (set of) participants based on the different resources they restake.
Team	Technical Architect, 1 FTE, 15 months Prototyping/Software Engineer, 1 FTE, 15 months Formal Methods Engineer, 1 FTE, 15 months Product Manager 0.3 FTE, 15 months
Documentation	The Minotaur paper (different scope but some approaches are reused)

TV-6. Light Client Infrastructure

Workstream Lead: Alex Slesarenko
Start Date: Aug 25
Duration (months): 9
Target SRL: 5
Target BRL: 3
2025 FTEs: 3.75
Intersect related Working Group: n/a
Product Roadmap Alignment: Developer / User Experience

Light clients aim to provide users with efficient protocols for managing wallets and participating in simple smart contracts, minimizing resource requirements and trust assumptions. The research explores trade-offs in light client infrastructure, including data retention, bandwidth, and processing limitations,

tailored for DApp development and mobile wallets. Safeguarding such data will likely require incentivized third-party providers, such as Blockfrost, which operate proprietary interfaces outside the blockchain's distributed system framework. In 2024, a draft paper was developed covering requirements, the light client landscape, and a protocol overview. Current work focuses on refining the protocol, leveraging blind signatures for construction. The novel blind signature scheme (without unlinkability) under consideration could introduce a new cryptographic primitive, enhancing the paper's significance and impact. This shift underscores the need for robust, decentralized solutions for light clients.

Problem: Many DApps would benefit from a decentralised and minimised light client solution to access data. At the moment, Mithril certificates provide concise certificates for the state of the chain, but it requires data providers to access the details of each transaction. Being able to provide a framework that enables data access in a trustful manner while minimizing data usage could simplify the deployment of solutions that rely on on-chain data, without compromising the trust and the decentralisation of the system.

Innovation: Secure and minimize data access for light-client, with clear incentive for the data providers

KPIs: TBC *

Application Area: Prototype the light client infrastructure, assess its viability and do a deep dive analysis of the incentive model. Provide clear security assumptions based on the current and potential future participation of Mithril and decentralised blockfrost.

Non-Functional Requirements: n/a

Market: Wallet and DApps

Business Model: n/a

Scope	Explore infrastructure for light-client, and how we can establish a trusted and incentivised relationship with third party data provider
Workplan *	TBC
Dependencies	Connection with the future development of Mithril and the decentralisation effort of Blockfrost
Deliverables	Documents: (i) Specification, (ii) Incentive analysis, (iii) Security analysis, (iv) Formalised technical requirements Software: (i) Working prototype
Innovation goal	Ease the deployment of dApps infrastructure that rely mainly on external services for their data layer
Team	Technical architect, 1 FTE, 9 months Prototyping/software engineer, 1.5 FTE, 9 months Formal methods engineer, 1 FTE, 9 months Cryptographer, 1 FTE, 9 months

	Developer Relations 0.5 FTE, 9 months
Documentation	Research draft documents

* At the time of publication, workstream planning is still in progress and subject to change.

3.5 Deliverables

Each year, IOR's goal is to generate a robust pipeline of at least 20 commercialization opportunities for the Cardano ecosystem at SRL2*, underpinned by comprehensive research papers and technical reports. From this funnel, we aim to validate and prioritize 6 key innovation opportunities for implementation on or for the benefit of Cardano that have been thoroughly validated at SRL4/5*. The outputs and deliverables outlined below build on IOR's historical track record over Cardano era's roadmap, and focus on reinforcing and advancing Cardano's leadership in the blockchain industry.

Fundamental Research

Since 2017 IOR has published over 200 research papers. This extensive body of work highlights the commitment to advancing blockchain technology for the benefit of Cardano. Papers published within this context can vary significantly in terms of length, complexity, and strategic importance, with the average paper taking at least two years to publish. This timeline is influenced by the peer review process, which can extend over several months and often requires multiple submission cycles, reflecting the high standards of academic publishing.

The research conference landscape is becoming increasingly competitive, particularly in areas critical to blockchain and cryptography. This intensifying competition highlights the importance of producing research that meets the highest standards of quality and relevance. In response, we are committed to delivering a consistent output of at least 20 research papers with accompanying technical artefacts each year across our research portfolio. This ensures that we continue to make meaningful contributions to the global research community and, more specifically, to the Cardano ecosystem.

Beyond generating high-quality research, IOR recognises the importance of visibility and impact within both academic and broader technology communities. Citations remain a key indicator of influence, and we are actively working to expand the reach and recognition of our work. To support this, we are strengthening our marketing efforts to ensure our research is not only published, but also effectively disseminated through relevant Cardano channels. Through these efforts, we aim to drive deeper engagement with our research, amplify its impact, and reinforce Cardano's position as a leader in blockchain innovation.

Technology Validation

The innovation deliverables include technology validation to SRL4/5* of 6 prototypes, technical reports and Community Improvement Proposals (CIPs) as a result of these workstreams. Please note workstreams starting in the second half of the year will be delivered the following year.

These technical reports will offer in-depth analyses and documentation of each emerging technology, along with the supporting methodologies essential for ongoing implementation by product teams within

the Cardano ecosystem. Each report will act as a foundation for future development, helping to inform the community and stakeholders of the implementation requirements. Accompanying prototypes will showcase the practical applications of these innovations, illustrating how theoretical advances can be transformed into real-world solutions.

In parallel, Cardano Problem Statements (CPSs) and Community Improvement Proposals (CIPs) form a central pillar of our innovation strategy. CIPs promote collaboration and transparency across the Cardano community, enabling community-driven enhancements to the platform. By submitting well-researched and strategically aligned CIPs, we aim to address key challenges and opportunities within the ecosystem—ensuring Cardano remains at the forefront of blockchain innovation.

3.6 Budget Justification

The $13.42M total budget proposed is to finance all activities across both academic research and technology validation with a total of 56.1 FTEs. This equates to an average of circa $239k per FTE (or $1,030 per day based on 232 working days per year) including all costs as outlined below, such as equipment, software licenses, server costs, any sub-contracting that may be required (for example to academic partners or third-party engineers), administration, travel, events, and program and portfolio management.

Research

The research departmental budget is circa $5.895M for a total of 27.5 FTEs in terms of labor resources. This is approximately $295k per workstream per year, at an average of circa 1.3 FTE, where it takes on average 2 years or more to publish a research paper.

Each of the 20 fundamental research workstreams requires a mix of academic experience that can include distributed systems, consensus, protocol design and security, applied cryptography, game theory, and formal specifications/verification. The resources allocated to each workstream can vary from 2-6 team members, includes all sub-contracting and strategic partnerships with universities, and typically includes the following roles:

(a) Chief Scientist - oversees research strategy, drives innovation, and academic excellence
(b) Professors - world-renowned experts in their field
(c) Senior Research Fellow - leads advanced research projects, mentors researchers, and publishes findings.
(d) Research Fellow - conducts specialized research, collaborates on projects, and contributes to publications.
(e) Researcher (Associates and PhDs) - pursues doctoral research, assists in studies, and develops expertise.
(f) Engineers - Research, Formal Method or Software - develops and implements technical solutions, supports research, and ensures software quality.

At the start of a research workstream the FTE scope can be very wide due to the high level of uncertainty, and as the workstream develops this is then narrowed as investigative directions are realized.

Innovation

The innovation departmental budget is $7,525,000 for a total of 28.6 FTEs in terms of labor resources. This is approximately $1.25M per technology validation workstream for 6-12 months of intensive effort.

Each of the 6 validation workstreams requires specific dedicated skill sets which might vary depending on development requirements (for example, not all require cryptographic knowledge). The resources allocated to each workstream typically range from 4.6 - 6 FTEs and includes the following roles:

(a) Product manager / Developer relationship - Develops product discovery, market fit, builds the use cases and identifies supporting customers
(b) Technical Architect - define and provide inputs on the prototype/target environment
(c) Prototyping engineer (software) - Prototyping, Modeling and Simulation Engineer(s)
(d) Applied Cryptographer - define and provide inputs on the cryptographic primitives implementation and benchmark
(e) Researcher liaison - author and support the team on additional research and paper publications
(f) Formal methods engineer - define formal models, specifications and executable models to be used in performance testing.

Technology Validation streams frequently occur over two calendar years. In this instance, funding is allocated to each stream on a pro-rata basis and any additional Technology Validation streams are proposed via the Intersect Product Committee.

3.7 Reporting

Reporting for Work Program 25 will follow a structured process, ensuring transparency and accountability across all workstreams. The portfolio of individual workstreams will be proposed through the relevant Technical Steering and Product Committees and will be shared with respective Working Groups and special interest groups. This collaborative approach invites feedback and input from a broad range of stakeholders, ensuring that the proposed workstreams are aligned with the strategic goals of the Cardano ecosystem.

The mid-year interim report will serve as a crucial checkpoint, providing a high-level update on workstream statuses including tasks and deliverables. This report will also highlight any minor change requests that have arisen. Major change requests, which could significantly impact the direction or scope of the workstreams, will be handled on a case-by-case basis, with decisions made in consultation with the relevant committees in a timely manner. The mid-year report will also play a vital role in clarifying and confirming the details of proposed innovation workstreams set to begin in the second half of the year.

At the end of the year, a comprehensive final report will be prepared, providing a detailed summary of all deliverables achieved throughout the year. This report will also include a thorough breakdown of associated final costs, offering a clear view of the financial and operational outcomes of the program. Together, these reports will ensure that the progress and results of the workstreams are clearly

communicated, and any necessary adjustments are made to maintain alignment with Cardano's strategic objectives.